CA92276-8603-02

PRIMERGY

スイッチブレード（1Gbps 36/8+2）（PG-SW111）
スイッチブレード（1Gbps 36/12）（PG-SW112）

スイッチユーザーズガイド

FUJITSU

本書をお読みになる前に

外国為替及び外国貿易法に基づく特定技術について

当社のドキュメントには「外国為替および外国貿易管理法」に基づく特定技術が含まれていることがあります。特定技術が含まれている場合は、当該ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

本書の内容について

このたびは、弊社の PRIMERGY スイッチブレード (1Gbps 36/8+2) ／PRIMERGY スイッチブレード (1Gbps 36/12) をお買い上げいただき、誠にありがとうございます。
本書は、本製品がスイッチモードに設定されている場合のコマンド使用方法を示した、スイッチユーザーズガイドのマニュアルです。なお、本文は英語で記載しています。
本書をよくお読みになり、正しい取り扱いをされますようお願いいたします。

■ 関連マニュアル

- PRIMERGY スイッチブレード(1Gbps 36/8+2)(PG-SW111)／PRIMERGY スイッチブレード (1Gbps 36/12) (PG-SW112) 取扱説明書
- PRIMERGY スイッチブレード (1Gbps 36/8+2) (PG-SW111)／PRIMERGY スイッチブレード (1Gbps 36/12) (PG-SW112) IBP ユーザーズガイド
- PRIMERGY スイッチブレード (1Gbps 36/8+2) (PG-SW111)／PRIMERGY スイッチブレード (1Gbps 36/12) (PG-SW112) スイッチコンフィグレーションガイド
- PRIMERGY スイッチブレード (1Gbps 36/8+2) (PG-SW111)／PRIMERGY スイッチブレード (1Gbps 36/12) (PG-SW112) IBP コンフィグレーションガイド

上記マニュアルは「PRIMERGY」ページの「マニュアル」(http://primeserver.fujitsu.com/primergy/manual.html) からご覧ください。

PRIMERGY ブレード･サーバ･システム

スイッチ取扱説明書

2010年12月版

目次

1	**重要な注意事項**	**21**
1.1	ボードについて	21
1.2	準拠性宣言	22
2	**序文**	**25**
2.1	イーサネット･コネクション･ブレードの機能	27
2.1.1	MAC アドレスによる機能	28
2.1.2	レイヤー2+の機能	29
2.1.3	スパニング･ツリー･プロトコル機能	33
2.1.4	イーサネット･コネクション･ブレードの管理機能	34
2.1.5	セキュリティ機能	38
2.1.6	QOS 機能	40
2.2	ハードウェアの説明	42
2.2.1	イーサネット･コネクション･ブレードのポート構成	42
2.2.2	イーサネット･ポート	43
2.2.3	LED の状態	44
2.2.4	サポートされる SFP+と SFP のベンダー一覧表	46
2.3	機能と利点	47
2.3.1	接続機能	47
2.3.2	性能	47
2.3.3	管理	48
2.4	表記規則	48
2.5	この手順書の対象ユーザー	48
2.6	テクニカル･データ	49
3	**ネットワーク計画**	**50**
3.1	スイッチングの紹介	50
3.2	用途例	51
3.2.1	バックボーン接続	51
3.2.2	VLAN 接続を作る	51
4	**ネットワーク接続を確立する**	**53**
4.1	1000BASE-T 機器に接続する	53
4.2	1000BASE-T ケーブル要件	54
4.2.1	既存 Cat5 ケーブルのケーブル･テスト	54
4.2.2	既存 Cat5 ケーブルを 1000BASE-T に調整する	54
4.2.3	1000BASE-T のピン割当て	55
5	**イーサネット･コネクション･ブレードを構成する**	**56**
5.1	概　要	56
5.2	イーサネット･コネクション･ブレードを接続する	57
5.3	イーサネット･コネクション･ブレードの起動と構成	59
5.4	端末を構成する	61
5.5	デバイスを起動する	62
5.6	ソフトウェア･ダウンロード	63
5.6.1	BootROM バック･ドア CLI から	63
5.6.2	オペレーション･コード CLI による	65
5.7	ソフトウェアの起動モードを切り替える	67
6	**スタック機能を理解する**	**68**
6.1	序文	68
6.2	スタック機能概要	69
6.3	スタック･マスターの選定プロセス	70
6.4	ファームウェアのアップグレードと配布プロセス	71
6.5	電源供給のポイント	72
6.6	スタック･メンバーのプロビジョニング	75

6.7 名前付けの仕組み ... 76
6.7.1 スイッチ名 ... 76
6.7.2 スタック内の名前付けとアドレス割当て ... 76

7 E-KEY 機能の特長 E-KEY ... 77

8 ウェブ・ベース管理インターフェイス ... 78
8.1 概　要 ... 78
8.1.1 メニュー・オプション ... 79
8.2 管理メニュー ... 82
8.2.1 情報 ... 82
8.2.1.1 インベントリ情報 ... 82
8.2.1.2 ARP キャッシュ ... 83
8.2.2 構成 ... 85
8.2.2.1 システム内容 ... 85
8.2.2.2 インバンド管理 ... 86
8.2.2.3 Out-of-Band管理 ... 88
8.2.2.4 Telnetセッション ... 89
8.2.2.5 Telnetクライアント・コンフィグ ... 90
8.2.2.6 シリアルポート ... 91
8.2.2.7 HTTP コンフィグ ... 93
8.2.2.8 DDNSコンフィグ ... 94
8.2.3 システム・ユーティリティー ... 95
8.2.3.1 すべての変更を保存する ... 95
8.2.3.2 システムのリセット ... 95
8.2.3.3 コンフィグをデフォルトに設定する ... 96
8.2.3.4 パスワードをデフォルトに設定する ... 96
8.2.3.5 Traceroute ... 97
8.2.3.6 Ping ... 98
8.2.4 ファイル管理 ... 100
8.2.4.1 スイッチへダウンロードする ... 100
8.2.4.2 スイッチからアップロードする ... 102
8.2.4.3 起動ファイル ... 103
8.2.4.4 ファイルを削除する ... 104
8.2.4.5 ファイルをコピーする ... 105
8.2.5 ユーザー管理 ... 106
8.2.5.1 ユーザー・アカウント ... 106
8.2.5.2 認証リスト・コンフィグ ... 108
8.2.5.3 認証リスト・サマリ ... 110
8.2.5.4 ユーザー・ログイン ... 111
8.2.5.5 ログイン・セッション ... 112
8.2.6 ロギング ... 113
8.2.6.1 バッファー・ログを構成する ... 113
8.2.6.2 コマンド・ロガーを構成する ... 113
8.2.6.3 コンソール・ログを構成する ... 114
8.2.6.4 ホストを構成する ... 115
8.2.6.5 シスログを構成する ... 116
8.2.6.6 バッファー・ログを見る ... 116
8.2.6.7 イベント・ログを見る ... 118
8.2.7 統計 ... 119
8.2.7.1 スイッチ・サマリ ... 119
8.2.7.2 スイッチの詳細 ... 120
8.2.7.3 ポート・サマリ ... 122
8.2.7.4 ポート詳細 ... 123
8.2.8 SNMP ... 127
8.2.8.1 コミュニティー・コンフィグ ... 127
8.2.8.2 トラップ・レシーバー・コンフィグ ... 129
8.2.8.3 トラップ・フラッグ ... 130
8.2.8.4 トラップ・ログ ... 131
8.2.8.5 サポートされるMIB ... 132
8.2.9 SNTP ... 133

8.2.9.1 グローバル･コンフィグ ... 133
8.2.9.2 グローバル･ステータス ... 134
8.2.9.3 サーバ･コンフィグ ... 136
8.2.9.4 サーバ･ステータス ... 137
8.2.9.5 現在時刻 ... 138
8.2.9.6 時間帯設定 ... 139
8.2.10 CDP ... 140
8.2.10.1 構成 ... 140
8.2.10.2 周辺情報 ... 141
8.2.10.3 統計 ... 142
8.2.11 LDP ... 143
8.2.11.1 グローバル･コンフィグ ... 143
8.2.11.2 インターフェイス･コンフィグ ... 144
8.2.11.3 インターフェイス･サマリを見る ... 145
8.2.11.4 統計を見る ... 146
8.2.11.5 ローカル情報を見る ... 147
8.2.11.6 ローカル･サマリを見る ... 149
8.2.11.7 遠隔情報を見る ... 150
8.2.11.8 リモート･サマリを見る ... 151
8.2.12 DHCP クライアント ... 152
8.2.12.1 DHCPクライアント識別子 ... 152
8.2.12.2 DHCP再起動 ... 153
8.2.12.3 DHCP6 再起動 ... 153
8.2.13 DNS リレー ... 153
8.2.13.1 DNSリレー･コンフィグ ... 153
8.2.13.2 ドメイン名コンフィグ ... 155
8.2.13.3 ネームサーバ･コンフィグ ... 156
8.2.13.4 DNSキャッシュ･サマリ ... 157
8.2.13.5 ホスト･コンフィグ ... 158
8.2.14 IPv6 ... 159
8.2.14.1 統計 ... 159
8.3 スイッチングのメニュー ... 163
8.3.1 転送データベース ... 163
8.3.1.1 構成 ... 163
8.3.1.2 検索 ... 164
8.3.2 ポート ... 165
8.3.2.1 構成 ... 165
8.3.2.2 サマリ ... 166
8.3.2.3 ミラーリング ... 168
8.3.3 VLAN ... 169
8.3.3.1 構成 ... 169
8.3.3.2 ステータス ... 172
8.3.3.3 ポートの構成 ... 173
8.3.3.4 Port Summary ... 174
8.3.3.5 構成をリセットする ... 175
8.3.4 プロトコルベースの VLAN ... 176
8.3.4.1 構成 ... 176
8.3.4.2 サマリーサマリー ... 177
8.3.5 IP サブネットベースの VLAN ... 178
8.3.5.1 構成 ... 178
8.3.5.2 サマリー ... 178
8.3.6 MAC ベースの VLAN ... 180
8.3.6.1 構成 ... 180
8.3.6.2 サマリー ... 181
8.3.7 GARP ... 182
8.3.7.1 グローバル･コンフィグ ... 182
8.3.7.2 ポートの構成 ... 183
8.3.7.3 ステータス ... 184
8.3.8 VTP ... 186
8.3.8.1 構成 ... 186
8.3.8.2 サマリー ... 188

8.3.9 IGMP スヌーピング 189
8.3.9.1 構成とステータス 189
8.3.9.2 インターフェイスの構成 190
8.3.9.3 VLAN構成 191
8.3.9.4 VLAN のステータス 192
8.3.10 IGMP スイッチスヌーピング･クエリア 193
8.3.10.1 構成 193
8.3.10.2 VLAN構成 194
8.3.10.3 VLAN 構成概要 195
8.3.10.4 VLAN ステータス 196
8.3.11 IGMP マルチキャスト静的グループ 197
8.3.11.1 構成 197
8.3.11.2 ステータス 198
8.3.12 マルチキャスト･ルータ 199
8.3.12.1 構成 199
8.3.12.2 統計 200
8.3.12.3 VLAN構成 201
8.3.12.4 VLAN 統計 202
8.3.13 MLD スヌーピング 203
8.3.13.1 構成とステータス 203
8.3.13.2 インターフェイスの構成 204
8.3.13.3 VLAN 構成 204
8.3.13.4 VLAN ステータス 205
8.3.14 MLD スヌーピング･クエリア 207
8.3.14.1 構成 207
8.3.14.2 VLAN構成 208
8.3.14.3 VLAN 構成概要 209
8.3.14.4 VLAN ステータス 210
8.3.15 MLD マルチキャスト静的グループ 211
8.3.15.1 構成 211
8.3.15.2 ステータス 212
8.3.16 MLD マルチキャスト･ルータ 213
8.3.16.1 構成 213
8.3.16.2 統計 214
8.3.16.3 VLAN構成 215
8.3.16.4 VLANの統計 216
8.3.17 ユニキャスト･転送データベース 217
8.3.17.1 MFDBテーブル 217
8.3.17.2 GMRPテーブル 218
8.3.17.3 IGMP スヌーピングテーブル 219
8.3.17.4 MLDスヌーピングテーブル 220
8.3.17.5 統計 221
8.3.18 ポート･チャネル 222
8.3.18.1 構成 222
8.3.18.2 ｽﾃｰﾀｽ 224
8.3.19 スパニング･ツリー 225
8.3.19.1 スイッチ構成/ステータス 225
8.3.19.2 CST 226
8.3.19.3 MST 228
8.3.19.4 CST ポート 229
8.3.19.5 MST ポート 231
8.3.19.6 統計 233
8.3.20 リンク･ステート 234
8.3.20.1 構成 234
8.3.20.2 ステータス 235
8.3.21 ポートのバックアップ 236
8.3.21.1 構成 236
8.3.21.2 ステータス 237
8.3.22 MAC フィルター 238
8.3.22.1 構成 238
8.3.22.2 サマリー 239

8.4 セキュリティ･メニュー 240
8.4.1 ポートアクセス制御 240
8.4.1.1 構成 240
8.4.1.2 ポート･コンフィグ 241
8.4.1.3 ポートステータス 243
8.4.1.4 ポート･サマリ 245
8.4.1.5 統計 246
8.4.1.6 ログイン 248
8.4.1.7 アクセス特権 248
8.4.1.8 アクセス･サマリ 249
8.4.2 ポート･セキュリティ 250
8.4.2.1 構成 250
8.4.2.2 インターフェイス･コンフィグ 250
8.4.2.3 静的MACアドレス 252
8.4.2.4 動的MACアドレス 252
8.4.2.5 バイオレーションステータス 253
8.4.3 RADIUS を構成する 254
8.4.3.1 構成 254
8.4.3.2 サーバ･コンフィグ 255
8.4.3.3 アカウンティング･サーバ･コンフィグ 257
8.4.4 RADIUS 統計 258
8.4.4.1 RADIUS 統計 258
8.4.4.2 サーバ統計 258
8.4.4.3 アカウンティング･サーバ統計 260
8.4.4.4 統計をクリアする 261
8.4.5 TACACS+ 262
8.4.5.1 コンフィグ 262
8.4.5.2 サーバ･コンフィグ 263
8.4.6 LDAP 264
8.4.6.1 構成 264
8.4.7 アクセス制御リスト 265
8.4.7.1 IPコンフィグ 265
8.4.7.2 IPサマリ 266
8.4.7.3 IP規則コンフィグ 267
8.4.7.4 MACコンフィグ 269
8.4.7.5 MACサマリ 270
8.4.7.6 MAC規則コンフィグ 270
8.4.7.7 ポート･コンフィグ 273
8.4.8 IP フィルター 275
8.4.8.1 構成 275
8.4.9 セキュア HTTP 276
8.4.9.1 構成 276
8.4.10 セキュア･シェル 277
8.4.10.1 構成 277
8.4.11 Denial-of-Service 278
8.4.11.1 構成 278
8.5 QoS Menu 280
8.5.1 差別化サービス 280
8.5.1.1 グローバル･コンフィグ 280
8.5.1.2 DiffServウィザード 282
8.5.1.3 クラス･コンフィグ 284
8.5.1.4 クラス･サマリ 286
8.5.1.5 ポリシー･コンフィグ 286
8.5.1.6 ポリシー･サマリ 288
8.5.1.7 ポリシー･クラス定義 288
8.5.1.8 ポリシー属性サマリ 290
8.5.1.9 サービス･コンフィグ 291
8.5.1.10 サービス･サマリ 292
8.5.1.11 サービス統計 293
8.5.1.12 サービス詳細統計 294
8.5.2 CoS 295

8.5.2.1 トラストモード ... 295
8.5.2.2 IP DSCPマッピング ... 296
8.5.2.3 プライオリティ・マッピング ... 297
8.5.2.4 インターフェイス ... 298
8.5.2.5 インターフェイス・キュー ... 299
8.5.2.6 インターフェイス・キュー・ステータス ... 300
8.6 スタック・メニュー ... 301
8.6.1 構成 ... 301
8.6.1.1 ユニット・コンフィグ ... 301
8.6.1.2 アーカイブ・コピー ... 303
8.6.2 情報 ... 304
8.6.2.1 サマリ ... 304
8.6.2.2 ポート・サマリ ... 305
8.6.2.3 ポート・カウンター ... 306
8.6.2.4 ポート・カウンターの詳細 ... 307

9 コマンド・レファレンス ... 308
9.1 CLI コマンド・フォーマット ... 308
9.2 CLI モード・ベースのトポロジー ... 309
9.3 システム情報と統計的コマンド ... 311
9.3.1 show arp ... 311
9.3.2 show calendar ... 311
9.3.3 show eventlog ... 312
9.3.4 show running-config ... 312
9.3.5 show sysinfo ... 313
9.3.6 show system ... 314
9.3.7 show hardware ... 314
9.3.8 show version ... 316
9.3.9 show tech-support ... 316
9.3.10 show loginsession ... 318
9.4 デバイス構成コマンド ... 319
9.4.1 インターフェイス ... 319
9.4.1.1 show interface status ... 319
9.4.1.2 show interface counters ... 321
9.4.1.3 show interface switch ... 328
9.4.1.4 interface ... 329
9.4.1.5 interface range ... 329
9.4.1.6 speed-duplex ... 330
9.4.1.7 negotiate ... 330
9.4.1.8 capabilities ... 332
9.4.1.9 storm-control flowcontrol ... 333
9.4.1.10 shutdown ... 334
9.4.1.11 MDI/MDIX ... 335
9.4.2 L2 MAC アドレスとマルチキャスト転送データベーステーブル ... 336
9.4.2.1 show mac-addr-table ... 336
9.4.2.2 show mac-addr-table count ... 337
9.4.2.3 show mac-addr-table interface ... 338
9.4.2.4 show mac-addr-table vlan ... 338
9.4.2.5 show mac-address-table gmrp ... 339
9.4.2.6 show mac-address-table igmpsnooping ... 341
9.4.2.7 show mac-address-table mldsnooping ... 341
9.4.2.8 show mac-address-table multicast ... 342
9.4.2.9 show mac-address-table stats ... 344
9.4.2.10 show mac-addr-table agetime ... 344
9.4.2.11 mac-addr-table aging-time ... 345
9.4.3 VLAN 管理 ... 346
9.4.3.1 show vlan ... 346
9.4.3.2 show vlan id ... 346
9.4.3.3 show vlan association mac ... 348
9.4.3.4 show vlan association subnet ... 349
9.4.3.5 show protocol group ... 350

9.4.3.6 show interface switchport ... 350
9.4.3.7 VLAN database ... 351
9.4.3.8 vlan ... 352
9.4.3.9 vlan name ... 352
9.4.3.10 vlan association mac ... 353
9.4.3.11 vlan association subnet ... 353
9.4.3.12 vlan makestatic ... 354
9.4.3.13 protocol group ... 354
9.4.3.14 switchport acceptable-frame-type ... 355
9.4.3.15 switchport ingress-filtering ... 357
9.4.3.16 switchport native vlan ... 357
9.4.3.17 switchport allowed vlan ... 359
9.4.3.18 switchport tagging ... 360
9.4.3.19 switchport priority ... 361
9.4.3.20 switchport protocol group ... 362
9.4.3.21 switchport forbidden vlan ... 364
9.4.4 GVRP and Bridge Extension (GVRP とブリッジ拡張) ... 365
9.4.4.1 show bridge-ext ... 365
9.4.4.2 show gvrp configuration ... 365
9.4.4.3 show gmrp configuration ... 366
9.4.4.4 show garp configuration ... 367
9.4.4.5 bridge-ext gvrp ... 368
9.4.4.6 bridge-ext gmrp ... 368
9.4.4.7 switchport gvrp ... 369
9.4.4.8 switchport gmrp ... 371
9.4.4.9 garp timer ... 372
9.4.5 VTP Commands (VTP コマンド) ... 378
9.4.5.1 show vtp counters ... 378
9.4.5.2 show vtp password ... 379
9.4.5.3 show vtp status ... 379
9.4.5.4 show vtp trunkport ... 380
9.4.5.5 vtp ... 381
9.4.5.6 vtp domain ... 381
9.4.5.7 vtp mode ... 382
9.4.5.8 vtp password ... 382
9.4.5.9 vtp pruning ... 383
9.4.5.10 vtp version ... 383
9.4.5.11 vtp trunkport ... 384
9.4.6 IGMP Snooping (IGMP スヌーピング) ... 385
9.4.6.1 コマンドを表示 ... 385
9.4.6.1.1 show ip igmp snooping ... 385
9.4.6.1.2 show ip igmp snooping mrouter ... 385
9.4.6.1.3 show ip igmp snooping ... 386
9.4.6.1.4 show ip igmp snooping static ... 387
9.4.6.2 構成コマンド ... 387
9.4.6.2.1 ip igmp snooping ... 387
9.4.6.2.2 ip igmp snooping groupmembershipinterval ... 388
9.4.6.2.3 ip igmp snooping interfacemode ... 388
9.4.6.2.4 ip igmp snooping mcrtrexpiretime ... 389
9.4.6.2.5 ip igmp snooping max-response-time ... 389
9.4.6.2.6 ip igmp snooping fast-leave ... 390
9.4.6.2.7 ip igmp snooping mrouter ... 391
9.4.6.2.8 set igmp ... 392
9.4.6.2.9 set igmp groupmembership-interval ... 392
9.4.6.2.10 set igmp maxresponse ... 393
9.4.6.2.11 . set igmp mcrtexpiretime ... 393
9.4.6.2.12 set igmp fast-leave ... 394
9.4.6.2.13 ip igmp snooping static ... 394
9.4.7 IGMP Snooping Querier (IGMP スヌーピング·クエリア) ... 395
9.4.7.1 コマンドを表示 ... 395
9.4.7.1.1 IGMP snooping querier global info ... 395

9.4.7.1.2 Display IGMP snooping querier vlan info ... 396
9.4.7.1.3 IGMP snooping querier detail information ... 397
9.4.7.2 構成コマンド ... 398
9.4.7.2.1 IGMP snooping querier admin mode ... 398
9.4.7.2.2 IGMP snooping querier address ... 398
9.4.7.2.3 IGMP snooping querier query-interval ... 399
9.4.7.2.4 IGMP snooping querier querier-expiry-interval ... 399
9.4.7.2.5 IGMP snooping query verion ... 400
9.4.7.2.6 IGMP snooping querier vlan admin mode ... 400
9.4.7.2.7 IGMP snooping querier vlan address ... 401
9.4.7.2.8 IGMP snooping querier vlan election mode ... 402
9.4.8 MLD スヌーピング ... 403
9.4.8.1 コマンドを表示 ... 403
9.4.8.1.1 show ipv6 mld snooping ... 403
9.4.8.1.2 show ipv6 mld snooping mroute ... 404
9.4.8.1.3 show ipv6 mld snooping mrouter interface ... 405
9.4.8.1.4 show ipv6 mld snooping mrouter vlan ... 405
9.4.8.1.5 show ipv6 mld snooping static 。 ... 406
9.4.8.1.6 show mac-address-table mldsnooping ... 406
9.4.8.2 構成コマンド ... 407
9.4.8.2.1 ip mld snooping ... 407
9.4.8.2.2 ipv6 mld snooping interfacemode ... 407
9.4.8.2.3 ipv6 mld snooping fast-leave ... 408
9.4.8.2.4 ipv6 mld snooping groupmembershipinterval ... 408
9.4.8.2.5 ipv6 mld snooping max-response-time ... 409
9.4.8.2.6 ipv6 mld snooping mcrtrexpiretime ... 409
9.4.8.2.7 ipv6 mldスヌーピングmrouterインターフェイス ... 410
9.4.8.2.8 ipv6 mld静的スヌーピング ... 410
9.4.8.2.9 set mld ... 411
9.4.8.2.10 set mld fast-leave ... 411
9.4.8.2.11 set mld groupmembership-interval ... 412
9.4.8.2.12 set mld maxresponseコマンド ... 412
9.4.8.2.13 set mld mcrtrexpiretime ... 413
9.4.9 MLD スヌーピングクエリア ... 414
9.4.9.1 コマンドを表示 ... 414
9.4.9.1.1 show ipv6 mld snooping querier ... 414
9.4.9.1.2 show ipv6 mld snooping querier vlan ... 415
9.4.9.1.3 MLDスヌーピングクエリアの情報のすべてを表示します ... 415
9.4.9.2 構成コマンド ... 417
9.4.9.2.1 ipv6 mld snooping querier ... 417
9.4.9.2.2 ipv6 mld snooping querier address ... 417
9.4.9.2.3 ipv6 mld snooping querier querier-interval ... 418
9.4.9.2.4 ipv6 mld snooping querier querier-expiry-interval ... 418
9.4.9.2.5 ipv6 mld snooping querier vlan ... 419
9.4.9.2.6 ipv6 mld snooping querier vlan ... 419
9.4.9.2.7 MLD snooping querier vlan election mode ... 420
9.4.10 ポートチャネル ... 421
9.4.10.1 show port-channel ... 421
9.4.10.2 show lacp interface ... 423
9.4.10.3 port-channel ... 423
9.4.10.4 port-channel adminmode all ... 424
9.4.10.5 port-channel linktrap ... 425
9.4.10.6 port-channel name ... 425
9.4.10.7 port-channel load-balance ... 426
9.4.10.8 adminmode ... 426
9.4.10.9 staticcapability ... 427
9.4.10.10 lacp ... 427
9.4.10.11 channel-group ... 428
9.4.10.12 delete-channel-group ... 429
9.4.11 ストームの制御 ... 430
9.4.11.1 show storm-control ... 430

9.4.11.2 storm-control broadcast ... 431
9.4.11.3 storm-control multicast ... 433
9.4.11.4 storm-control unicast ... 434
9.4.11.5 switchport broadcast packet-rate ... 435
9.4.11.6 switchport multicast packet-rate ... 436
9.4.11.7 switchport unicast packet-rate ... 437
9.4.12 L2 プライオリティ ... 438
9.4.12.1 show queue cos-map ... 438
9.4.12.2 queue cos-map ... 439
9.4.13 ポートミラー ... 440
9.4.13.1 show port-monitor session ... 440
9.4.13.2 port-monitor session ... 440
9.4.13.3 port-monitor session mode ... 441
9.5 静的 MAC フィルタリングコマンド ... 442
9.5.1 コマンドを表示 ... 442
9.5.1.1 show mac-addr-table static ... 442
9.5.2 構成コマンド ... 443
9.5.2.1 macfilter ... 443
9.5.2.2 macfilter addsrc ... 443
9.5.2.3 macfilter addsrc all ... 444
9.6 管理コマンド ... 445
9.6.1 ネットワークコマンド ... 445
9.6.1.1 show ip interface ... 445
9.6.1.2 show ip redirects ... 445
9.6.1.3 show ip filter ... 446
9.6.1.4 mtu ... 446
9.6.1.5 interface vlan ... 447
9.6.1.6 ip address ... 447
9.6.1.7 ip default-gateway ... 448
9.6.1.8 ip address protocol ... 448
9.6.1.9 enable ip filter ... 449
9.6.1.10 ip filter ... 449
9.6.1.11 show oob ... 450
9.6.1.12 oob ip ... 450
9.6.1.13 oob gateway ... 451
9.6.1.14 oob protocol ... 451
9.6.2 シリアルインターフェイスコマンド ... 452
9.6.2.1 show line console ... 452
9.6.2.2 line console ... 453
9.6.2.3 baudrate ... 453
9.6.2.4 exec-timeout ... 453
9.6.2.5 password-threshold ... 454
9.6.2.6 silent-time ... 454
9.6.2.7 login local ... 455
9.6.2.8 terminal-length ... 455
9.6.2.9 show pager ... 456
9.6.2.10 pager ... 456
9.6.2.11 show displaymode ... 457
9.6.2.12 displaymode ... 457
9.6.3 Telnet セッションコマンド ... 458
9.6.3.1 telnet ... 458
9.6.3.2 show line vty ... 459
9.6.3.3 line vty ... 459
9.6.3.4 server enable ... 460
9.6.3.5 exec-timeout ... 460
9.6.3.6 password-threshold ... 461
9.6.3.7 maxsessions ... 461
9.6.3.8 sessions ... 462
9.6.3.9 terminal-length ... 462
9.6.3.10 telnet sessions ... 463
9.6.3.11 telnet maxsessions ... 463

9.6.3.12 telnet exec-timeout 464
9.6.3.13 show telnet 464
9.6.4 SNMP サーバコマンド 465
9.6.4.1 show snmp 465
9.6.4.2 show trapflags 465
9.6.4.3 snmp-server sysname 467
9.6.4.4 snmp-server location 467
9.6.4.5 snmp-server contact 468
9.6.4.6 snmp-server community 468
9.6.4.7 snmp-server host 470
9.6.4.8 snmp-server enable traps 471
9.6.5 SNMP トラップコマンド 474
9.6.5.1 show snmptrap 474
9.6.5.2 snmp trap link-status 475
9.6.5.3 snmptrap <name> <ipaddr> 476
9.6.5.4 snmptrap ipaddr 476
9.6.5.5 snmptrap mode 477
9.6.6 HTTP コマンド 478
9.6.6.1 show ip http 478
9.6.6.2 ip javamode 478
9.6.6.3 ip http port 479
9.6.6.4 ip http server 479
9.6.6.5 ip http secure-port 480
9.6.6.6 ip http secure-server 480
9.6.6.7 ip http secure-protocol 481
9.6.6.8 ip http session 481
9.6.6.9 ip http secure-session 482
9.6.7 セキュア Shell (SSH) コマンド 483
9.6.7.1 show ip ssh 483
9.6.7.2 ip ssh 483
9.6.7.3 ip ssh protocol 484
9.6.7.4 ip ssh maxsessions 484
9.6.7.5 ip ssh timeout 485
9.6.8 DHCP クライアントコマンド 486
9.6.8.1 ip dhcp restart 486
9.6.8.2 ip dhcp client-identifier 486
9.6.9 DHCPv6 クライアントコマンド 487
9.6.9.1 ipv6 address protocol 487
9.6.9.2 ipv6 dhcp6 restart 487
9.6.9.3 oob protocol 488
9.6.9.4 oob protocol dhcp6 restart 488
9.6.10 ドメインネームサーバリレーコマンド 488
9.6.10.1 Showコマンド 488
9.6.10.1.1 show hosts 488
9.6.10.1.2 show dns 489
9.6.10.2 show dns cache 490
9.6.10.3 設定コマンド 491
9.6.10.3.1 ip hosts 491
9.6.10.3.2 clear hosts 492
9.6.10.3.3 ip domain-name 492
9.6.10.3.4 ip domain-list 493
9.6.10.3.5 ip name-server 494
9.6.10.3.6 ip domain-lookup 494
9.6.10.3.7 clear domain-list 495
9.6.10.3.8 clear dns 495
9.6.10.3.9 clear dns cache 496
9.6.10.3.10 clear dns counter 496
9.6.11 動的 DNS クライアントコマンド 497
9.6.11.1 ddns client 497
9.6.11.2 show ddns 498
9.6.12 IPv6 コマンド 499

9.6.12.1 show ipv6 interface ... 499
9.6.12.2 show ipv6 traffic ... 499
9.6.12.3 clear ipv6 statistics ... 502
9.6.13 CDP コマンド ... 503
9.6.13.1 show cdp ... 503
9.6.13.2 show cdp neighbors ... 503
9.6.13.3 show cdp traffic ... 504
9.6.13.4 cdp ... 504
9.6.13.5 cdp run ... 504
9.6.13.6 cdp timer ... 506
9.6.13.7 cdp holdtime ... 506
9.6.14 LLDP コマンド ... 506
9.6.14.1 show lldp ... 506
9.6.14.2 show lldp interface ... 507
9.6.14.3 show lldp statistics ... 508
9.6.14.4 show lldp remote-device ... 509
9.6.14.5 show lldp remote-device detail ... 510
9.6.14.6 show lldp local-device ... 511
9.6.14.7 show lldp local-device detail ... 512
9.6.14.8 lldp notification ... 513
9.6.14.9 lldp notification-interval ... 513
9.6.14.10 lldp receive ... 513
9.6.14.11 lldp transmit ... 514
9.6.14.12 lldp transmit-mgmt ... 514
9.6.14.13 lldp transmit-tlv ... 515
9.6.14.14 lldp timers ... 515
9.7 システムログ管理コマンド ... 517
9.7.1 Show コマンド ... 517
9.7.1.1 show loggingコマンド ... 517
9.7.2 show logging buffered ... 518
9.7.3 show logging traplog ... 519
9.7.3.1 show logging hosts ... 520
9.7.4 設定コマンド ... 521
9.7.4.1 logging buffered ... 521
9.7.4.2 logging console ... 522
9.7.4.3 logging host ... 522
9.7.4.4 logging syslog ... 524
9.7.4.5 clear logging buffered ... 525
9.8 スクリプト管理コマンド ... 526
9.8.1 script apply ... 526
9.8.2 script delete ... 526
9.8.3 script list ... 526
9.8.4 script show ... 527
9.9 システムユーティリティ ... 528
9.9.1 clear ... 528
9.9.1.1 clear arp ... 528
9.9.1.2 clear traplog ... 528
9.9.1.3 clear eventlog ... 529
9.9.1.4 clear logging buffered ... 529
9.9.1.5 clear config ... 530
9.9.1.6 clear pass ... 530
9.9.1.7 clear counters ... 530
9.9.1.8 clear dns counter ... 531
9.9.1.9 clear dns cache ... 531
9.9.1.10 clear cdp ... 532
9.9.1.11 clear vlan ... 532
9.9.1.12 enable passwd ... 533
9.9.1.13 clear igmp snooping ... 533
9.9.1.14 clear mld snooping ... 534
9.9.1.15 clear port-channel ... 534
9.9.1.16 clear port-security dynamic ... 535

9.9.1.17 clear ip filter 535
9.9.1.18 clear ipv6 statistics 536
9.9.1.19 clear dot1x statistics 536
9.9.1.20 clear radius statistics 536
9.9.1.21 clear tacacs 537
9.9.1.22 clear lldp 538
9.9.1.23 clear vtp statistics 538
9.9.2 copy 539
9.9.2.1 copy upload File 539
9.9.2.2 copy download File 540
9.9.2.3 copy running-config startup-config 541
9.9.2.4 copy clibanner 541
9.9.2.5 copy file running-config 542
9.9.3 delete 543
9.9.4 dir 544
9.9.5 whichboot 545
9.9.6 boot-system 546
9.9.7 ping 547
9.9.7.1 ping <host> count [size] 547
9.9.7.2 ping ipv6 548
9.9.7.3 ping ipv6 interface 548
9.9.8 traceroute 549
9.9.9 logging cli-command 550
9.9.10 calendar set 550
9.9.11 reload 551
9.9.12 Configure 551
9.9.13 disconnect 552
9.9.14 hostname 552
9.9.15 pager 553
9.9.16 do 554
9.9.17 quit 554
9.10 スパニングツリー・コマンド 555
9.10.1 Show コマンド 555
9.10.1.1 show spanning-tree 555
9.10.1.2 show spanning-tree interface 556
9.10.1.3 show spanning-tree vlan 557
9.10.1.4 show spanning-tree mst 557
9.10.1.5 show spanning-tree summary 561
9.10.1.6 show spanning-tree brief 562
9.10.2 Config コマンド 563
9.10.2.1 spanning-tree 563
9.10.2.2 spanning-tree protocol-migration 563
9.10.2.3 spanning-tree configuration 564
9.10.2.4 spanning-tree mode 565
9.10.2.5 spanning-tree bpdu forwarding 565
9.10.2.6 spanning-tree edgeport 566
9.10.2.7 spanning-tree uplinkfast 569
9.10.2.8 spanning-tree loopguard 569
9.10.2.9 spanning-tree forward-time 571
9.10.2.10 spanning-tree hello-time 571
9.10.2.11 spanning-tree max-age 572
9.10.2.12 spanning-tree max-hops 572
9.10.2.13 spanning-tree mst 573
9.10.2.14 spanning-tree port mode 579
9.10.2.15 spanning-tree edgeport 580
9.11 ユーザアカウント管理コマンド 581
9.11.1 Show コマンド 581
9.11.1.1 show users 581
9.11.1.2 show users authentication 582
9.11.2 Config コマンド 583
9.11.2.1 username 583

9.11.2.2 username snmpv3 authentication ... 583
9.11.2.3 username snmpv3 encryption ... 584
9.11.2.4 username defaultlogin ... 585
9.11.2.5 username login ... 585
9.12 LinkState コマンド ... 586
9.12.1.1 show link state ... 586
9.12.2 Config コマンド ... 587
9.13 port-backup コマンド ... 589
9.13.1 show port-backup ... 589
9.13.2 Config コマンド ... 590
9.14 SNTP コマンド ... 592
9.14.1 Show コマンド ... 592
9.14.1.1 show sntp ... 592
9.14.1.2 show sntp client ... 593
9.14.1.3 show sntp server ... 594
9.14.2 Config コマンド ... 595
9.14.2.1 sntp broadcast client poll-interval ... 595
9.14.2.2 sntp client mode ... 595
9.14.2.3 sntp client port ... 596
9.14.2.4 sntp unicast client poll-interval ... 596
9.14.2.5 sntp unicast client poll-timeout ... 597
9.14.2.6 sntp unicast client poll-retry ... 597
9.14.2.7 sntp server ... 598
9.14.2.8 sntp clock timezone ... 599
9.14.2.9 sntp multicast client poll-internal ... 599
9.15 Security コマンド ... 600
9.15.1 Show コマンド ... 600
9.15.1.1 show users authentication ... 600
9.15.1.2 show authentication ... 600
9.15.1.3 show authentication users ... 601
9.15.1.4 show dot1x ... 601
9.15.1.5 show dot1x detail ... 602
9.15.1.6 show dot1x statistics ... 603
9.15.1.7 show dot1x summary ... 603
9.15.1.8 show dot1x users ... 605
9.15.1.9 show radius-servers ... 605
9.15.1.10 show radius ... 606
9.15.1.11 show radius accounting ... 606
9.15.1.12 show radius statistics ... 608
9.15.1.13 show tacacs ... 609
9.15.1.14 show port-security ... 610
9.15.2 Config コマンド ... 612
9.15.2.1 authentication login ... 612
9.15.2.2 username defaultlogin ... 613
9.15.2.3 username login ... 613
9.15.3 Dot1x コマンド ... 614
9.15.3.1 dot1x initialize ... 614
9.15.3.2 dot1x default-login ... 614
9.15.3.3 dot1x login ... 615
9.15.3.4 dot1x system-auth-control ... 615
9.15.3.5 dot1x user ... 616
9.15.3.6 dot1x port-control ... 616
9.15.3.7 dot1x max-req ... 617
9.15.3.8 dot1x re-authentication ... 618
9.15.3.9 dot1x re-reauthenticate ... 618
9.15.3.10 dot1x timeout ... 619
9.15.4 Radius コマンド ... 620
9.15.4.1 radius accounting mode ... 620
9.15.4.2 radius-server host ... 620
9.15.4.3 radius-sever key ... 621
9.15.4.4 radius-server retransmit ... 622

9.15.4.5 radius-server timeout 622
9.15.4.6 radius-server msgauth 623
9.15.4.7 radius-server primary 623
9.15.5 TACACS+コマンド 624
9.15.5.1 tacacs host 624
9.15.5.2 tacacs key 626
9.15.5.3 tacacs timeout 627
9.15.6 port-security コマンド 628
9.15.6.1 port-security 628
9.15.6.2 port-security max-dynamic 628
9.15.6.3 port-security max-static 629
9.15.6.4 port-security mac-address 629
9.15.6.5 port-security mac-address move 630
9.15.6.6 port-security violation shutdown 630
9.15.7 LDAP コマンド 631
9.15.7.1 show ldap 631
9.15.7.2 ldap ip 631
9.15.7.3 ldap port 632
9.15.7.4 ldap baseDN 632
9.15.7.5 ldap racName 633
9.15.7.6 ldap racDomain 633
9.16 差別化サービスコマンド 634
9.16.1 一般コマンド 635
9.16.1.1 diffserv 635
9.16.1.2 Classコマンド 636
9.16.2 クラスコマンド 637
9.16.2.1 class-map 638
9.16.2.2 no class-map 639
9.16.2.3 class-map rename 640
9.16.2.4 match any 640
9.16.2.5 match class-map 641
9.16.2.6 no match class-map 642
9.16.2.7 match dstip 642
9.16.2.8 match dstl4port 643
9.16.2.9 match ip dscp 644
9.16.2.10 match ip precedence 645
9.16.2.11 match ip tos 646
9.16.2.12 match protocol 647
9.16.2.13 match srcip 647
9.16.2.14 match srcl4port 648
9.16.2.15 match cos 649
9.16.2.16 match destination-address mac 649
9.16.2.17 match ethertype 650
9.16.2.18 match secondary-cos 650
9.16.2.19 match secondary-vlan 651
9.16.2.20 match source-address mac 651
9.16.2.21 match vlan 652
9.16.3 Policy コマンド 653
9.16.3.1 assign-queue 653
9.16.3.2 drop 654
9.16.3.3 mirror 654
9.16.3.4 redirect 655
9.16.3.5 conform-color 655
9.16.3.6 mark cos 656
9.16.3.7 mark ip-dscp 657
9.16.3.8 mark ip-precedence 657
9.16.3.9 police-simple 658
9.16.3.10 class 658
9.16.3.11 no class 659
9.16.3.12 policy-map 659
9.16.3.13 policy-map rename 660

9.16.4 Service コマンド........ 661
9.16.4.1 service-policy........ 661
9.16.4.2 no service-policy........ 662
9.16.5 Show コマンド........ 663
9.16.5.1 show diffserv........ 663
9.16.5.2 show diffserv service........ 664
9.16.5.3 show diffserv service brief........ 665
9.16.5.4 show class-map........ 666
9.16.5.5 show policy-map........ 667
9.16.5.6 show policy-map interface........ 668
9.16.5.7 show service-policy........ 669
9.17 ACL コマンド........ 670
9.17.1 Show コマンド........ 670
9.17.1.1 show mac access-lists........ 670
9.17.1.2 show mac access-lists........ 671
9.17.1.3 show ip access-lists........ 671
9.17.1.4 show access-lists interface........ 672
9.17.2 Config コマンド........ 673
9.17.2.1 mac access-list extended........ 673
9.17.2.2 mac access-list extended........ 673
9.17.2.3 mac access-list........ 674
9.17.2.4 mac access-group in........ 675
9.17.2.5 access-list........ 676
9.17.2.6 no access-list........ 677
9.17.2.7 ip access-group........ 677
9.18 CoS コマンド........ 678
9.18.1 Show コマンド........ 678
9.18.1.1 show queue cos-map........ 678
9.18.1.2 show queue ip-dscp-mapping........ 679
9.18.1.3 show queue trust........ 680
9.18.1.4 show queue cos-queue........ 681
9.18.2 Config コマンド........ 682
9.18.2.1 queue cos-map........ 682
9.18.2.2 queue ip-dscp-mapping........ 684
9.18.2.3 queue trust........ 685
9.18.2.4 queue cos-queue min-bandwidth........ 686
9.18.2.5 queue cos-queue strict........ 687
9.18.2.6 queue cos-queue traffic-shape........ 688
9.19 Stack コマンド........ 689
9.19.1 Show コマンド........ 689
9.19.1.1 show switch........ 689
9.19.1.2 show switch stack port........ 690
9.19.1.3 show stack port counter statistic........ 690
9.19.2 Config コマンド........ 692
9.19.2.1 スイッチのプライオリティを設定する........ 692
9.19.2.2 switch provision........ 692
9.19.2.3 switch movemanagement........ 693

10 SNMP を使用する........ 694
10.1 対応 MIB........ 695
10.2 MIB オブジェクトにアクセスする........ 697
10.3 対応トラップ........ 700

1 重要な注意事項

この取説は装置のそばに保管すること。第三者に装置を渡す場合、この取説もともに渡すこと。 この頁を注意してよく読み、装置を開梱する前に情報のメモを取ること。 まず装置を開いてからでないとスイッチ・ブレードにはアクセスできない。この取扱説明書の「重要な注意事項」の章にある安全中事項に従うこと。 部品は稼動中に極めて高温になる。装置を取り扱う際は部品に触らないこと。 火傷の危険がある。 設置中に装置が損傷 した場合保証は無効となる。

1.1 ボードについて

装置または部品と部品に実装されている導電部品を損傷しないために、これらを挿入または取外すときは注意深く行うこと。 ボードが真っ直ぐｽﾛｯﾄに装着され、部品または部品にある導電部品、または他の部品を損傷しないことに十分注意すること。 ボードを交換するときはロック機構 (キャッチ、センタリング・ピン等)を丁寧に取り扱うこと。

装置を浮かすときに鋭利な物(ドライバー等)を使用してはならない。 静電により損傷しやすいデバイス(ESD)を実装したボードは表記のラベルにより識別できる。 ESDを実装したボードを取り扱うときは、いかなる事情があっても必ず次の項目に従うこと:

– 作業前には必ず静電気を取り除く(たとえば、接地された物に触る等)こと。
– 設備や工具には静電蓄積が無いこと。
– ESDを実装したボードを挿入したり取外す前に主電源から電源プラグを抜くこと。
– ESD付きボードは常にボードの縁を持つこと。
– ESDを装備したボードにあるピンや導電部品には触らないこと。

1.2 準拠性宣言

FCC Class A準拠性

この装置はFCC (連邦通信委員会)規則パート15による「クラスA」デジタル装置に課される限界値に準拠することが試験により実証済みであり、(カナダ干渉発生機器規格のすべての要件に合格している。 当該限界値は住宅での接地の際有害な干渉から適格な保護を提供するために設計されている。 この設備は無線周波エネルギーを発生し、使用し、放射し、厳密に指示通りに設置され使用されない場合、無線通信に有害な干渉を発生することがある。しかし、特定の設置形態では干渉が発生しないという保証は無い。 この設備がラジオやテレビの受信に有害な干渉を発生しうる場合、 これはラジオやテレビの電源を入れたり切ったりするとわかるー、次のうち一つまたはそれ以上の措置を講じて干渉を是正すること。

– 受信アンテナの方向を変えるまたは場所を移す。
– この設備と受信機をさらに離す。
– この設備を受信機が接続されているのとは別の回路のコンセントに接続する。
– 補助が必要な場合受信機の販売店かラジオやテレビの経験豊かな技術者に相談すること。

富士通テクノロジー・ソリューションズは、この設備の未許諾変更または富士通テクノロジー・ソリューションズが指定したものとは異なる接続コードや設備で代替または接続することから発生したラジオやテレビの干渉からは免責される。当該の未承諾変更、代替または接続に起因する干渉の是正はユーザーの責任である。

RJ-45 接続には非シールド・ツイストペア・ケーブル(UTP) ー 10Mbps接続にはカテゴリ3以上、 100Mbps接続にはカテゴリ5以上、1000Mbpsにはカテゴリ5または5e ー を使用できる。



この設備を取り扱う際の静電放電を防止するため静電防止用リスト・ベルトを着用するまたは他の適格な措置を取ること。

インダストリ・カナダ規格クラスA

このデジタル装置は、カナダ通信省ICES003 の「デジタル装置」干渉発生装置規格に規定されるデジタル装置からの無線ノイズ発生に対するクラスA限界値を超えない。

日本VCCIクラスA

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

電磁波干渉および安全性(EEC)に関するCEマーク準拠性宣言

この情報技術設備は欧州委員会指令 89/336/EECによる電磁両立性に関する加盟国法律の適合化および一定の電圧限界値以内で使用される電気機器に関する指令 73/23/EECおおびその修正指令 93/68/EECの要件に準拠する。当該指令との準拠性評価には次の規格を使用した：

- **無線周波数干渉の放出：**
  - **EN 55022:1998 による限界値クラスA**
  - **EN 61000-3-2/2006 による高調波放出限界値クラスA**
  - **EN 61000-3-3/1995 による低電圧電源系の電圧変動やムラの制限**
- **電磁波耐性：**
  - **EN 55024:1998 による製品群規格**
  - **EN 61000-4-2:1995 による静電放電 (接触放電許容値： ±8 kV、空中放電： ±8 kV)**
  - **EN 61000-4-3:1995 による無線周波数電磁場許容値 (1 kHz AM 80%変調による 80 - 1000MHz： 3 V/m)**
  - **EN 61000-4-4:2004 による高速過渡/バースト電圧 (AC/DC電源： ±1 kV、データ:/信号ライン： ±0.5 kV)**
  - **EN 61000-4-5:1995 によるサージ電磁波耐性試験(AC/DC線間: ±1 kV、AC/DCライン対接地: ±2 kV)**
  - **無線周波数場により誘導される伝導妨害による電磁波耐性： EN 61000-4-6:1996 による(1 kHz AM 80% 変調による 0.15 - 80 MHz: 3 V/m)**
  - **EN 61000-4-8:1993 による電源周波数電磁場電磁波耐性試験(50Hz周波数で1A/m)**
  - **EN 61000-4-11:1994 による電圧降下、短時間の中断、 および電圧変動に対する 耐性 試験(>95% 減少 @10 ms、30% 減少 @500 ms、 >95% 減少 @5000 ms)**
- **VD:**
  - **EN 60950 (A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)**



RF-45 ポートに電話用ジャックコネクタを差し込まないこと。 これはポートを損傷する場合がある。 ポートは電話線には使用禁止である。

台湾BSMI クラスA

警告使用者：這是甲類的資訊產品，在居住的
環境中使用時，可能會造成射頻干擾，在這種
情況下，使用者會被要求採取某些適當的對策。

オーストラリアAS/NZS 3548 (1995) - クラスA



2 序文

PRIMERGY BX900 ブレード･サーバはモジュール構成サーバであり、最大 18 個のサーバ、 8 個のコネクション･ブレード(基本仕様に 6 個のコネクション･ブレードが含まれ、別に 2 個はオプション)、2 個の管理モジュール (MMB)を一体化している。イーサネット･コネクション･ブレード･モジュールはプライマジーBX900 ブレード･サーバ･システムにネットワーキングとスイッチ機能を提供します。管理モジュールはPRIMERGY BX900 ブレード･サーバの一点制御点である。
PRIMERGY BX900 ブレード･サーバは、PRIMERGY BX900 GbEコネクション･ブレード 36/8+2 スタック(PG-SW111)とPRIMERGY BX900 GbEコネクション･ブレード 36/12 (PG-SW112)からなる 2 種類のイーサネット･コネクション･ブレードを内蔵している。

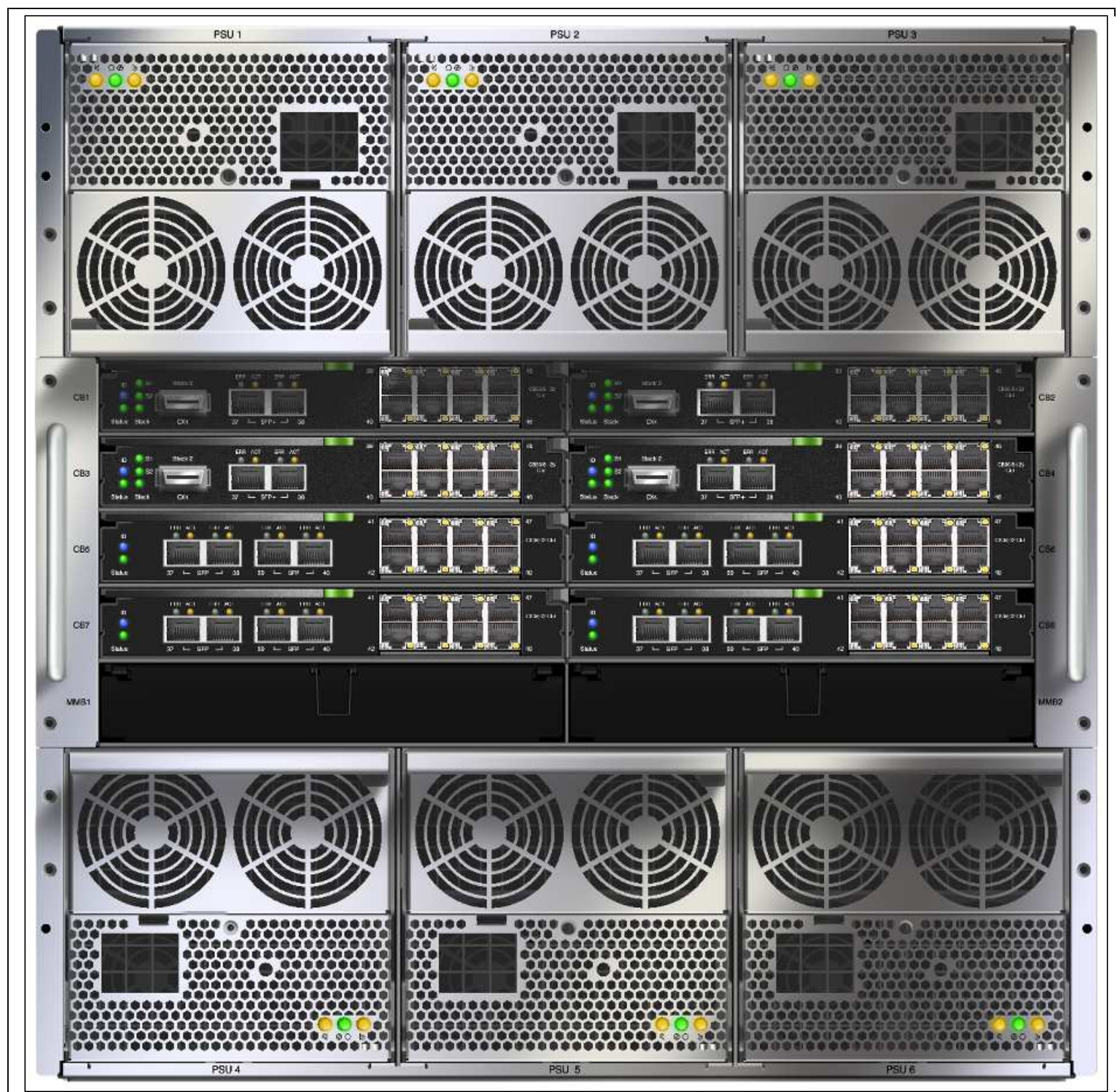
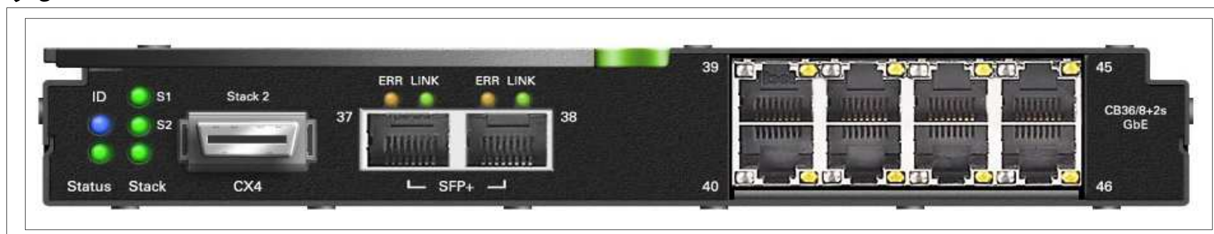


図: BX900 ブレード･サーバの背面

イーサネット･コネクション･ブレードは 10Uの次世代型ブレード･サーバのために設計された。 コネクション･ブレードには次に示す 2 種類ある。

a) PG-SW111 は 10GbE の SFP が 2 つある 46 ポート 1GbE でアップリンク･レイヤー2 スイッチを備 えたスタック接続できるイーサネット･コネクション･ブレードです。イーサネット･コネクション･ブレードの構成は中央部に 36 個のダウンリンク･ポート、さらにアップリンク･ポートには RJ45 コネクタによる 8 個の 1GbE および 2 個の 10GbE SFP+からなる。2 つの HiGig/HiGig+ポートがあり、ひとつは中間面に接続され、もうひとつはスタック接続機能を提供するイーサネット･コネクション･ブレードの実際のパネルにあります。スタック部は最大 8 個の PG-SW111 スイッチをサポートする



図： PRIMERGY BX900 GbEコネクション･ブレードの 36/8+2 スタック(PG-SW111) 前面

b) PG-SW112 は 48 ポート 1GbE、 4 個の 1GbE SFP+ アップリンク･レイヤー2+イーサネット･コネクション･ブレードである。 イーサネット･コネクション･ブレードの構成は中央部に 36 個のダウンリンク･ポート、さらにアップリンク･ポートには RJ45 コネクタによる 8 個の 1GbE および 4 個の 1GbE SFP からなる。

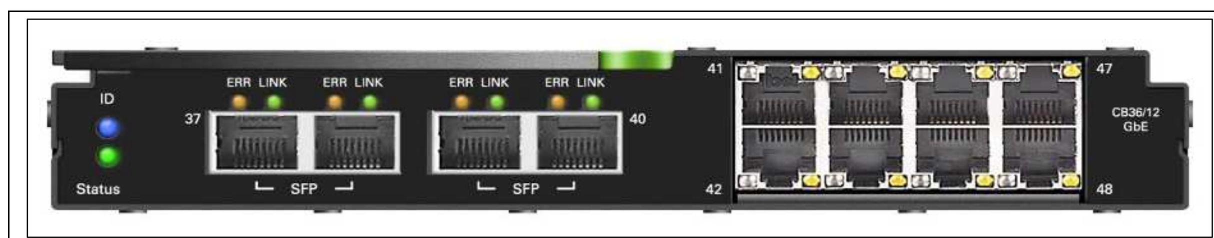


図: PRIMERGY BX900 GbEコネクション･ブレードの 36/12 (PG-SW112) 前面

装置への端末接続はMMBボードのみが司る。 デバッグと管理のためには、イーサネット･コネクション･ブレードのUARTバスがMMBボードに接続されている。 MMBボードは同時に 1 個のみのコネクション･ブレードを管理対象として選択できる。 このイーサネット･コネクション･ブレードはMMB管理用インバンド管理インターフェイスにもなる。

2.1 イーサネット･コネクション･ブレードの機能

このイーサネット･コネクション･ブレードは性能を強化する多くの高度機能を提供する。 マルチキャスト･フィルタリングは実時ネットワーク･アプリケーションをサポートする。 ポート･ベースのタグ付きVLAN、さらに自動GVRP VLAN登録サポートによりトラフ ィックの安全性とネットワーク帯域の効率的使用が可能である。 QoSプライオリティ･キューイングは ネットワーク全体で実時マルチメディア･データを移動する際の遅延を最小限にできる。フロー制御によりポートの飽和が引き起こす障害によるパケット損失は 無い。 さらにブロードキャスト･ストーム抑制によりブロードキャスト･ トラフィックがネッ トワークを飲み込むのを防ぐ 次に管理機能をいくつかサマリーして紹介する。

Head of Line Blocking

Head of Line Blocking(HOL)は、同一出口ポートのバッファに競合するトラフィックの遅延とフレーム損失を生起させる。 Head of Line Blockingはパケットを順に並べ、キュー先頭パケットはキュー最後のパケットより先に転送される。

フロー制御サポート (IEEE 802.3X)

フロー制御はより高速なデバイスによるパケット送信を抑制して低速デバイスが高速デバイスと通信できるようにする。 伝送はバッファー･オーバーフローを防止するため一時的に停められる。

バックプレッシャ ･サポート

半二重リンクでは、受信ポートは追加的トラフィックにはリンクが利用できないようにリンクを占有してバッファー･オーバーフローを防止する。

ジャンボフレーム･サポート

ジャンボフレームはMTUサイズが 9Kバイトまでのフレームであり、より少ないフレームを使用して同じデータを搬送するためネットワーク利用率が高まる。 この機能の最大の利点とは伝送オーバーヘッドとホスト処理オーバーヘッドの削減である。 フレーム数が少ないと入出力の中断が少なくなる。 この機能はサーバ間転送に主として使用される。

MDI/MDIXサポート

イーサネット･コネクション･ブレードはRJ-45 ポートに接続されたケーブルがクロスまたは ストレートかを自動検出する。端末用標準配線は媒体依存インターフェイス(MDI)であり、ハブおよびスイッチ用標準配線はMDIX (Media-Dependent Interface with Crossover)として周知である。

自動ネゴシエーション

自動ネゴシエーションによりイーサネット･コネクション･ブレードは動作モードを報知できる。 自動ネゴシエーションは 2 点間リンク部分を共有する 2 個のデバイスの間の情報交換さらにデバイスの伝送機能を最大限に活用するよう両デバイスを自動構成する手段となる。

2.1.1 MACアドレスによる機能

MACアドレス容量サポート

イーサネット･コネクション･ブレードはPG-SW112/PG-SW111 に最大 8K/16K個のMACアドレスをサポートする。 イーサネット･コネクション･ブレードはシステム用に特定のMACアドレスをリザーブする。

静的**MAC**登録項目

MAC登録項目は受信フレームから学習する代わりにブリッジング･テーブルに自分で入力できる。 これらのユーザー定義入力はエイジングとは無関係であり、リセットと再起動の際にも保持される。

自己学習型**MAC**アドレス

イーサネット･コネクション･ブレードは受信パケットからのMACアドレス自動学習を可能にする。 MACアドレスはブリッジング･テーブルに保存される。

MACアドレス自動エイジング

所定時間MACアドレスからトラフィックが来ない場合このMACアドレスは無効化される。このためブリッジング･テーブルはオーバーフローしない。

ポート・セキュリティ

ポート･セキュリティは未認証ユーザーがネットワークにアクセスするのを防止する。 この機能により当該ポートを通してネットワークにアクセスを承認されるデバイスに割当てるMACアドレス･リストを各ポートは学習できる。このポートで受信されたパケットはすべて認証リストにあるソース･アドレスを持つ必要があり、これがない場合落とされる。ポート･セキュリティはデフォルトではすべてのポートで無効化されているが、ポート毎に有効化できる。

アドレス・フィルタリング

このコネクション･ブレードはCPUポートに入るすべてのトラフィックのパケット･フィルターとなり、管理ネットワークに潜在的に転送またはルートされる。 パケット･フィルターは規則/パターンにより、あるパターンに合えばパケットを破棄し、あるパターンに合えばパケットを転送する 2 組のパターンから成る。

MACマルチキャスト・サポート

マルチキャスト･サービスは限定されたブロードキャスト･サービスであり、情報配信を 1 対多および多対 1 の接続により可能にする。レイヤー2 マルチキャスト･サービスでは 1 個のフレームが特定マルチキャスト･アドレスに宛てられ、そこからこのフレームのコピーが関連ポートに送信される。

2.1.2 レイヤー2+の機能

IGMP スヌーピング/MLD スヌーピング

IGMPスヌーピングはIGMPフレームがワークステーションから上流マルチキャスト・ルーターへイーサネット・コネクション・ブレードにより転送される際このフレームの内容を検査する。 フレームによりイーサネット・コネクション・ブレードはマルチキャスト・セッションのために構成されたワークステーションとマルチキャスト・フレームを送り出しているマルチキャスト・ルーターを識別する。

ポート・ミラーリング

ミラー・ポートはプローブ・ポートで送信および受信されたパケットともにモニターする。 イーサネット・コネクション・ブレードでは複数のプローブ・ポートと 1 個のミラー・ポートをサポートする。 ミラー・ポートはすべてのプローブ・ポートのパケットをパケットが落とされるかに関わらずすべてモニターする。 プローブ・ポートとミラー・ポートはIBP管理機能から設定できる。 プローブ・ポートとミラー・ポートの設定時、すべてのパケットが正しく反映されるように両ポートを同速度に構成しなければならない。 物理ポートとポートチャネル・ポートをプローブ・ポートとしてもよい。

ブロードキャスト・ストーム制御

ストーム制御によりIPパケット・スイッチング量を制限できる。理由は高速度と連続的トラフィックがネットワークを充満させることがあるからである。ストーム制御の仕組みはパケットがネットワーク上の他の部分を充満しないようにすることである。ブロードキャスト、マルチキャスト、およびユニキャストの転送速度がサポートされています。ユーザーはブロードキャスト、マルチキャスト、ユニキャストのフレームで 64、128、256、512 pps(毎秒パケット)の 4 つの異なる転送速度が利用できます。設定された転送速度を超えるトラフィックはすべてイーサネット・コネクション・ブレードでは破棄されます。この機能はデフォルトの環境設定では無効化されています。

VLANをサポートする機能

イーサネット・コネクション・ブレードは 1000 までのVLANと 4094 までのVLAN IDをサポートします。バーチャルLANは、物理的な場所やネットワークの接続ポイントに拘わらず同じコリジョン・ドメインを共有するネットワーク・ノードの集合です。イーサネット・コネクション・ブレードはIEEE 802 .1Q規格に基づいてタグ付けされたVLANをサポートします。 VLANグループのメンバーは、GVRP経由で動的に設定されるか、またはポートが特定のグループのVLANに手動で割り当てられることが可能です。これによりイーサネット・コネクション・ブレードはあるユーザーが割り当てられたVLANグループへのトラフィックを制限することができます。ネットワークをVANに分割することでユーザーは次のことができますイーサネット・コネクション・ブレードはあるユーザーが割り当てられたVLANグループへのトラフィックを制限することができます。ネットワークをVANに分割することでユーザーは次のことができます

a) フラットネットワークでの性能を著しく悪化させるブロードキャスト・ストームを解消できます。

b) 手動でネットワーク接続を変更しなければならないというよりむしろ、どのポートへの V LAN のメンバー登録も遠隔で設定することによりノードの変更と移動についてのネットワーク管理を簡略化できます。

c) ルータやレイヤー3 スイッチを使って別々の VLAN 間で接続が設定されている場所を除いて、元となる VLAN へのすべてのトラフィックを制限してデータのセキュリティーを提供できます。

VLANのサポート

VLANは単一のブロードキャスト・ドメインから成るスイッチポートの集合です。パケットはVLANタグに基づくか入口ポートとパケット内容の組み合わせに基づくVLANへ属するものとして識別されます。 共通の属性を共有するパケットは同じVLANにグループ分けできます。

a) ポートベースの VLANs

ポートベースのVLANはVLANへ入ってくるパケットを入口ポートに基づいて識別します。フレームはそのフレー

ムが着信するスイッチポートのみに基づいてVLANへ割り当てられます。特定のポートで受信されたフレームはすべて同じVLANに割り当てられます。

b) プロトコールベースの VLAN

VLANの識別ルールはデータリンク・レイヤー(レイヤー2)のプロトコル同定で定義されます。プロトコルベースのVLANは異なるレイヤー3 プロトコールへのレイヤー2 のトラフィックを分離します。すべてのフレームはそれが実行されているプロトコル、例えばIP、IPX、ARPなどにしたがって異なるVLANへ割り当てられます。たとえば、ユーザーはIPプロトコル上で実行されているフレームをあるVLANへ割り当て、IPX上で実行されているフレームは別のVLANへ割り当てることができます。

c) MAC アドレスペースの VLAN

MACアドレスベースのVLANでは、あるステーションのMACアドレスはあるVLANへ割り当てられます。それぞれのスイッチはMACアドレスとそれに対応するVLANの登録メンバーの割り当てテーブルを維持します。送信元または送信先MACアドレスがパケットがどのVLANへ渡されるかを決定します。

d) IP サブネットベースの VLAN 末端ステーションの IP サブネットアドレスを VLAN へ再マッ ピングするサポートをします。

802.1Q VLANタグ付け完全準拠

IEEE 802.1Qは仮想ブリッジLANのアーキテクチャ、VLANにより提供されるサービス、 当該サービスの供給に関わるプロトコルとアルゴリズムを定義する。 この規格に含まれる重要な要件は必要とするサービス・クラス (QoS)のタグ値(0-7)でフレーム を印せることである。

GVRP のサポート

GARP VLAN 登録プロトコール(GVRP)はIEEE 802.1Qに準拠したVLANプルーニングと 802.1Qのトランクポートにダイナミックの VLANの生成を提供します。GVRPが有効であると、イーサネット・コネクション・ブレード・モジュールは活発に内在しているスパニングツリー・プロトコル・トポロジーの一部であるすべてのポートでVLANのメンバーを登録し伝播させます。

GMRP プロトコール

GARP マルチキャスト登録プロトコル(GMRP)は、 IGMPスヌーピングに似た不自然なマルチキャスト・フラッディングを提供する包括的な属性登録プロトコルのアプリケーションです。GMRPとGARPはIEEE 802.1pで定義される業界標準のプロトコルです。GMRPは、ブリッジと端末ステーションが同じLANセグメントに付けられたMACアドレスを含むメンバー登録情報を動的に登録することを許可し、その情報が拡張されたフィルタリングサービスをサポートするブリッジLANのすべてのブリッジに伝播させます。GMRPの運用はGARPに提供されるサービスを当てにしています。GMRPソフトウェアのコンポーネントはイーサネット・コネクション・ブレードとホスト上で実行されます。ホスト上ではGMRPは主としてIGMPとともに使用されます: ホストのGMRPソフトウェアはホストのレイヤー3 IGMP制御パケットのレイヤー2 バージョンを発生させます。イーサネット・コネクション・ブレードはホストからレイヤー2 とレイヤー3 のIGMPトラフィックの両方を受信します。スイッチは抑制するため受信したGMRPトラフィックを使います。

VLAN トランキングプロトコール

VLANトランクプロトコル(VTP)はスイッチ化ネットワークの管理を削減します。ユーザーがあるVTPサーバ上の新しいVLANを構成する際、そのVLANはそのドメインのすべてのスイッチを通じて分配されます。これはいたるところの同じLANを構成する必要を削減します。サーバモード、クライアントモード、透明モード、ゼロVTPモードを含む 4 つのモードがサポートされています。

VTPはネットワーク基盤に広がったVLANの追加、削除、名前変更を管理することでVLAN環境設定の整合性を維持するレイヤー2 のメッセージングプロトコルです。VTPは二重のVLAN名、間違ったVLANタイプ仕様、そしてセキュリティ妨害といった多くの問題を生む原因となる環境設定ミスや不整合性を最小限にします。ユーザーはひとつのネットワークで 1～1005 のVLANを管理するためにVTPを使うことができます。 (VTPバージョン 1 とバージョン 2 は 1025 ～4094 のVLANをサポートしていません。)

VTPを使えばユーザーはひとつのマスタースイッチで環境設定を変更でき、その変更を同じVTP

ドメインとネットワークの他のすべてのスイッチに自動的に伝達させることができます。

リンクアグリゲーション

最大 6 個のメンバーポートを用いて 1 本の集約化リンクを定義し、単一のリンク集約化グループ(LAG)を形成できる。これで可能になる機能：

- **物理リンク障害時の耐障害性保護**
- **より広い帯域接続**
- **帯域粒度の向上**
- **広帯域サーバ接続性**

イーサネット・コネクション・ブレードは次の項目をサポートする：

- **アップリンクポート用に 6 トランクグループとダウンリンクポート用に 12 トランクグループまで(サポートします)(同じスイッチブレードに接続されたひとつのサーバブレードに 2 つのポートを結合する可能性だけでなく、ダウンリンクポートのためのLAGも提供されます。)**
- **構成可能規則による負荷分散：MACによるものとIPによるもの**

LAGは全二重動作に設定された等速度のポートから構成される。LAGの性能を強化するため、フロー制御をLAGに対しても有効化できる。

リンクアグリゲーションとLACP

LACPはリンク上のポイント通信を使用して動的にさまざまなリンクをアグリゲートし、現状のシステムペア間の最大アグリゲートを構成する。 LACPはシステム内でアグリゲート対象リンクへのポートの集約を自動的に決めたり、構成、結合、監視する。

フェイルオーバー伝搬サポート

ブレードサーバは二重ポートのネットワーク・インターフェイス・コントローラで、LANのチーミング機能とともにNIC管理プログラムを使う場合にはLAN冗長ポートを実現します。スイッチ時間を短縮してLAN冗長ポートの迅速な障害迂回を実現するために、フェイルオーバー伝播機能がPG-SW111 とPG-SW112 で導入されましたが、これはアップリンクポートが(物理的ポートとポートチャンネルのポートを含めて)LAN冗長ポートの切替を速くします。フェイルオーバーの状態にはリンクステータスも含まれます。

ポートバックアップ

ポートのパックアップ機能は冗長なアップリンクポート用にイーサネット・コネクション・ブレードでサポートされています。2 つのポートはひとつのグループに関連づけられています。2 つのポートはアクティブとバックアップポートの役割を果たします。リンクアップがアクティブポートと設定される場合バックアップポートは無効化されます。もし、リンクダウンがアクティブポートと設定されればバックアップポートに設定された方は有効になります。グループの 2 つのポートはグループが有効になる前は全部リンクアップなので、アクティブに設定された方は「アクティブ」になります。物理ポートとポートチャネルのポートがバックアップポートになる可能性もあります。(注記:この場合には、ポートチャンネルのメンバーはイーサネット・コネクション・ブレードのアップリンクポートでなければなりません設定された方は「アクティブ」になりやすいです。物理ポートとポートチャネルのポートがバックアップポートになる可能性もあります。(注記:この場合には、ポートチャンネルのメンバーはイーサネット・コネクション・ブレードのアップリンクポートでなければなりません。)

LLDP (リンク·レイヤー復元プロトコル)

LLDPはベンダーに中立のレイヤー2 プロトコルでネットワークデバイスがローカルネットワークでその識別と機能を通知ることを許可します。

IEEE 802.1AB リンク·レイヤー·ディスカバリー·プロトコル(LLDP)と呼ばれているこれは、拡張するLANによる環境設定問題に解決策を提供する新標準です。LLDPはスイッチ、ルーター、及び、無線LANアクセスポイントなどのイーサネットネットワークデバイスが自己情報をネットワークの他のノードへ公表したり自己発見する情報を保存するための標準的な方法を具体的に定義します。LLDPはすべての 802 メディアで実行されます。このプロトコルはデータリンクのレイヤーでのみ実行され、異なるネットワークレイヤープロトコルを実行している 2 つのシステムがお互いを認知できるようにします。

CDP (シスコ·ディスカバリー·プロトコル)

CDPはルーター、ブリッジ、アクセスとコミュニケーションサーバ、及び、スイッチを含むすべてのシスコ製装置で実行されるメディアとプロトコルに非依存のプロトコルです。CDPを使えば、ユーザーはスイッチに直接接続されたすべてのシスコ

のデバイスに関する情報を閲覧できます。 さらにCDPはネイティブVLANとポート通信設定の不一致を検出します。

ネットワーク管理アプリケーションはCDPにより周辺のシスコのデバイスのデバイスタイプとSNMPエージェントのアドレスを抽出できます。この機能はSNMPのクエリーを周辺デバイスへ送るアプリケーションを有効化します。CDPによってネットワーク管理アプリケーションは既知のデバイスの周辺特に低いレイヤー及び透過的なプロトコルを実行している周辺のデバイスを発見できます。CDPはデータリンクレイヤーでのみ実行されます。イーサネット・コネクション・ブレードはスイッチ機能のファームウェアでCDPv2 機能をサポートします。シスコのデバイスはCDPパケットを決して転送しません。新しいCDP情報が受信されるとシスコのデバイスは古いCDP情報を破棄します。イーサネット・コネクション・ブレードはスイッチ機能のファームウェアでCDPv2 機能をサポートします。

2.1.3 スパニング・ツリー・プロトコル機能

スパニング・ツリー・プロトコル(STP)

スパニングツリープロトコル(STP, IEEE 802.1D) – このプロトコルは、2 つ以上の冗長接続を 1 対のLANセグメントの間に生成して耐故障性を強化します。 セグメントの間に多重物理的パスがあると、このプロトコルは単一のパスを選び他のすべてを無効化してネットワークのどの 2 つのステーション間に 1 つのみルートを確保します。これがネットワークループが構成を防ぎます。しかし、通信パスがなんらかの理由で機能しなくなれば代替のパスがアクティベイトされて接続を維持します。

IEEE 802.1w 高速スパニングツリー

高速スパニングツリープロトコル(RSTP, IEEE 802.1w) – このプロトコルは、ネットワーク・トポロジー変化の収束時間を古いIEEE 802.1D STP規格で要求されていた数値の約 10%を減らすことができます。これはSTPを完全に置換するものと意図されていますが、もし、接続デバイスからSTPプロトコルメッセージを検出すればポートをSTPに準拠したモードに自動的に再構成することで古い標準を実行しているスイッチとも相互運用することができます。

IEEE 802.1s マルチプル・スパニングツリー

IEEE 802.1s マルチプル・スパニングツリー - IEEE 802.1sはIEEE Std 802.1Qに対する補完であり、VLANブリッジが、仮想ブリッジLAN内で潜在的に異なるパス上を流れる異なるVLANに属するトラフィックを提供するマルチプル・スパニングツリーを提供します。 802.1sはVLAN毎にスパニングツリーをサポートします。

ファーストリンク

STPは収束するのに 30～60 秒かかる可能性があります。この時間にSTPは可能性のあるループを検出し、時間を与えてステータスの変化が伝播すること、関連するイーサネット・コネクション・ブレード・モジュールが応答することを許してしまいます。30～60 秒は多くのアプリケーションにとっては長すぎる反応時間と考えられます。ファーストリンクのオプションはこの遅延をバイパスし、転送ループが発生しないネットワークトポロジーで使用します。

アップリンクファースト

アップリンクファーストは直接リンクの失敗後、高速な収束を提供し、アップリンクグループを使う冗長レイヤー2 のリンク間で読み込みのバランスを取ります。アップリンクグループはレイヤー2 インターフェイス(VLAN毎)の集合であり、その中の 1 つのみが随時転送機能を果たします。具体的には、アップリンクグループは(転送する)ルート・ポートと自己ループするポートを除いた妨害されたポートの集合とで構成されています。アップリンクグループは現在転送中のリンクが故障した時のために代替パスを提供します。

ループガード

STPループガード機能はループ(STPループ)を転送するレイヤー2 をさらに防御します。冗長なトポロジーのSTPブロッキングポートが誤って転送状態へ移行すると、STPループを生成します。物理的に冗長なトポロジー(必ずしもSTPブロッキングポートでなく)のポートのひとつがもはやSTP BPDUを受信しなくなるからです。STPはポートの役割に基づいてBPDUを常に受信または送信することに依存しながら運用されます。指定されたポートがBPDUを送信し、指定されないポートがBPDUを受信します。

物理的に冗長なトポロジーのポートのうちひとつがもはやBPDUを受信しなくなれば、STPはトポロジーが非ループと判断します。最終的には、代替またはバックアップポートからのブロッキングポートは指定されて転送状態へ移行します。こうして生成される状況がループです。

ループガード機能は追加的なチェックを行います。もしBPDUが指定されないポートでは受信されず、ループガードが有効であれば、そのポートはリスニング/ラーニング/フォワーディングの状態ではなく、STPループの一貫性のないブロッキング状態へ移行させられます。ループガード機能がなければ、そのポートは指定されたポートの役割を担います。 そのポートがSTP転送状態へ移り、ループが構成されます。

2.1.4 イーサネット･コネクション･ブレードの管理機能

PRIMERGY BX900 イーサネット･コネクション･ブレードはｺﾝｿｰﾙ･ポートまたは、 SNMP、TELNEtまたはHTTPプロトコルによりネットワークを介して管理できる。

管理操作で使用する各種のファイル:

a) BX900 イーサネット･コネクション･ブレードで使用する 3 種類のファイルがある:

- BootROMイメージ: 起動時にローダーが呼び出すイメージ。 POST(起動時自己診断) としても知られる。
- 設定ファイル： このファイルはシステム設定情報を保存する。
- 操作コード： システム起動後に実行される、実行時イメージとしても知られる。

b) フラッシュメモリの容量により、PRIMERGY BX900 は操作コードと BootROM イメージに各 2 個のコピー、設定ファイルでは 10 個のコピーのみサポートする。

c) イーサネット･コネクション･ブレード･モジュールのデュアルモードは PRIMERGY　BX900 でサポートされていて、ユーザーは電力再利用の後 CLI コマンドを通じてスイッチと IBP の間でイーサネット･コネクション･ブレードの機能を変更することができます。

管理ファイルの複製

PRIMERGY BX900 は以上 3 種類のファイルを次の方法でコピーできる。

1) ローカルファイルからローカルファイルへのコピー: PRIMERGY BX900 は既存のローカル設定ファ イルを別のローカルファイルにコピーできる。既存ローカル操作コードの別のローカルファイルへのコピーは禁止される。

2) リモート TFTP/FTP サーバからローカルファイルへのコピー: PRIMERGY BX900 は設定ファイル または操作コードのリモート･サーバからローカルファイルへのダウンロードをサポートする。

3) ローカルファイルからリモート･サーバへ: PRIMERGY BX900 は既存のローカル設定ファイルの リモート･サーバへのアップロードをサポートする。

4) 実行コンフィグからローカルファイルへのコピー:

5) 実行コンフィグからリモート TFTP/FTP サーバへ.

6) ローカルファイルから実行コンフィグへのコピー。

7) リモート TFTP/FTP サーバから実行コンフィグへのコピー。

起動ファイルを選択する

デフォルト起動構成と実行イメージとして使用される起動ファイルとして 10 個の設定ファイルから 1 ファイル、2 個の操作コードのコピーから 1 ファイルを選択でき、他の設定ファイルと操作コードはバックアップのために使用される。

構成をファイルに保存する

実行中の構成を今後使用するためにファイルに保存できる。新たに保存されたこの設定ファイルを後で起動ファイルに選ぶことができる。または、この保存された設定ファイルをリモート･サーバにアップロードしてバックアップできる。

プロビジョン

PRIMERGY BX900 では設定ファイルを選択してシステムを構成できる。 システムを構成するには 2 つのタイミングがある： 起動時と実行時である。

8) 起動時: 設定ファイルを起動のために選択する。

9) 実行時: 新たな設定ファイルを選択して、システム実行中でもシステムを構成でき、システム再起動は必要だが自動的に適用される。 この機能はコマンド･ライン･インターフェイスのみで利用できる。

SNMPアラームとトラップ･ログ

システム･ログ･イベントには重大度コードとタイムスタンプが含まれる。イベントはSNMPトラップとしてトラップ･レシーバ･リストに送られる。

SNMPバージョン 1、バージョン 2、バージョン 3

UDP/IPプロトコルによる簡易ネットワーク管理プロトコル（SNMP）システムへのアクセスを制御する ために、コミュニティー登録リストが定義され、この登録各項目はコミュニティー文字列およびアクセス特権から構成される。 SNMPセキュリティには読み出しのみとRead･Writeと 2 つのレベルがある。

ウェブによる管理

ウェブによる管理を用いてどのウェブ･ブラウザからでもシステムを管理できる。システムには埋め込みウェブサーバ(EWS)が含まれ、これはHTML頁のサーバとなり、これを通してシステムを監視、構成できる。システムはウェブによる入力を構成コマンド、MIB変数設定、他の管理関連設定に内部で変換する。

設定ファイルのダウンロードとアップロード

イーサネット･コネクション･ブレードの構成は設定ファイルに保存される。設定ファイルはシステム全体とポート別のイーサネット･コネクション･ブレード構成を含む。システムでは設定ファイル 10 個までがサポートされる。

スクリプト･ファイルの生成、ダウンロード、アップロード、適用

イーサネット･コネクション･ブレード構成の設定はテキストファイルとして保存され操作できるスクリプト･ファイルに保存できる。スクリプト･ファイルには、設定ファイルがコマンド･ライン･インターフェイス･コマンドの集合として表記される。スクリプト･ファイルはリモート･サーバとの間でダウンロード、アップロードともに可能であり、ダウンロードしたスクリプト･ファイルはコマンド･ライン･インターフェイス･コマンドによりシステムに適用できる。

TFTP/FTP　一般的なファイル転送プロトコル

イーサネット･コネクション･ブレードはTFTP/FTPによる起動イメージ、操作コード(実行時イメージ)、設定ファイルのアップロードとダウンロードをサポートする。

遠隔監視

遠隔監視（RMON）はSNMPを拡張したものである。(ネットワーク･イーサネット･コネクション･ブレード管理と監視を可能にするSNMPに対して)包括的なネットワーク･トラフィック監視機能を提供する。RMONは現在および過去のMACレイヤー統計と制御オブジェクトを定義する標準MIBであり、実時情報をネットワーク全体から取得することを可能にする。

コマンド・ライン・インターフェイス

コマンド・ライン・インターフェイス(CLI)の構文と動作は業界標準に準拠する。CLIは必須要素とオプション要素から構成される。CLIインタープリターはコマンドとキーワードを補完できるためユーザーを補助し、タイプを短くできる。

シスログ

シスログはリモート・サーバ・セットにイベント通知を送ることを可能にするプロトコルである。リモート・サーバにはイベント通知を保存でき、監視および直接対処できる。重要なイベントの通知を実時で送信し、これらのイベントの記録を事後的に使用するため保存できるという複数の機構が実装されている。

SNTP

簡易ネットワーク・タイム・プロトコル (SNTP)精確なネットワーク

イーサネット・コネクション・ブレードのクロック・タイム同期化をミリ秒精度で可能にする。時間同期化はネットワークSNTPサーバが行う。 ストラムが時間ソースを定義する。

ストラムは参照クロックからの距離を定義する。ハイストラムであればあるほど(0 に近づくほど)、クロックの精度は高い。イーサネット・コネクション・ブレードはDHCPサーバから取得されたSNTPサーバの使用をサポートして情報が呈示されるとクロックを同期化する。

BOOTPクライアント

BOOTP(ブートストラップ・プロトコル)はデバイスが起動すると保存されたパラメータを持続的に使用する代わりに、ネットワークにIPアドレスを動的に割当てるために使用される。BOOTPを使用するには、BOOTPサーバを立上げテーブルにデバイスのIPアドレスとMACアドレスを定義する必要がある。デバイスが起動すると、BOOTP要求を送り出しBOOTPサーバからIPアドレスを取得し、プロトコル・スタックを開始する。

DHCP/DHCPv6 クライアント

DHCP(動的ホスト構成プロトコル)はIPネットワーク上の個々のコンピュータにDHCPサーバから構成を展開する、特に、このサーバは各コンピュータが情報を要求するまでは個々のコンピュータについては精確な情報を持たない。 DHCPはBOOTPに基づいており、一部の下位互換性を保持する。 主な相違点は、BOOTPがサーバ・データベースにホスト情報を手動で予 め構成するよう設計されている一方、DHCPは新たに接続されたホストにネットワーク・アドレスと構成を動的に割当てることを可能にする。さらに、DHCPではリースメカニズムによりネットワーク・アドレスの復元と再割当てができる。

DNSクライアント

DNSプロトコルはホスト名をIPアドレスにマッピング可能な分散データベースであるドメイン・ネーム・システム(DNS)を制御する。スイッチ上でDNSを設定するときは、IPアドレスのためのホスト名をたとえばピング、Telnet 、トレイスルート等のすべてのIPコマンドおよび関連するTelnet をサポートする操作 で代用できます。ドメイン名を追跡するためIPではドメイン・ネーム・サーバというコンセプトが定義されており、これにはIPアドレスに対応させた名前のキャッシュ(すなわちデータベース)がある。ドメイン名とIPアドレスを対応させるには、まずホスト名を定義し、ネットワークにあるネームサーバを指定してからDNSを有効化しなければならない。

DDNS クライアント

これでホスト名とそのIPアドレスを、指定されたDDNSサーバに対応づけてDNSを解決できる。

IPv6 転送と**IPv6** サポート

IPv6 とは"インターネット・プロトコルのバージョン 6"を略記したものである。IPv6 はIETFが設計した次世代型プロトコルであり、現在のバージョンのインターネット・プロトコルである、IPバージョン 4 ("IPv4")を置換する。IPv6 は利用可能なIPv4アドレスの数に限界があるといったIPv4の問題を解決する。 さらにルーティングやネットワークの自動構成等ではIPv4 に多くの改善を追加する。 IPv6 はIPv4 を徐々に置換することが期待されており、推移期間中は両方が共存する。

管理用**IPv6 IP**アドレス

イーサネット・コネクション・ブレードのIPv6IPアドレスはMACアドレスをもとに自動的に計算される。

管理ポート用デフォルト・ゲートウェイ

システムでは 1 個のデフォルト・ゲートウェイのみサポートされる。インバンド管理インターフェイスまたはOut-of-band(OOB)管理インターフェイスのためにデフォルト・ゲートウェイを、 1 つだけ割当てることができる。インバンド管理用ゲートウェイが設定されていれば、それはイ ンバンド 管理 のみに有効である。 ゲートウェイをOut-of-band(OOB)管理にも設定しよう とすると、 インバンド 管理用ゲートウェイがすでに設定されていて二個構成できないというエラー・ メッセー ジが表示される。 Out-of-band(OOB)管理用ゲートウェイが設定されていれば、それはOut-of-band (OOB)管理インターフェイスのみに有効である。 ここでもインバンド管理用 ゲートウェイを構成しようとすると、対応するエラー・メッセージが表示される。

これら 2 個の管理ポートのうち 1 個をDHCPサーバからIPアドレスを取得するように構成すれば、DHCPサーバから取得されるデフォルト・ゲートウェイは既存のゲートウェイを上書きする。すなわち、デフォルト・ゲートウェイは、DHCPサーバによりIPアドレスとデフォルト・ゲートウェイの割当が完了すれば、DHCPを使用するように構成される管理ポートには常に有効化される。

2.1.5 セキュリティ機能

SSL

セキュア・ソケット・レイヤー(SSL)アプリケーション・レベルのプロトコルであり、非公開性、認証、データの完全性によりセキュリティが確立されたデータのやりとりを可能にする。これは証明書および公開鍵とシークレット鍵を使用する。現在はSSLバージョン 3 とTLSバージョン 1 がサポートされる。

SSH

セキュア・シェル(SSH)はプロトコルであり、イーサネット・コネクション・ブレードにセキュリティが確立した遠隔接続を可能にする。 現在はSSHバージョン 1 とバージョン 2 がサポートされる。 SSH サーバ機能によりSSHクライアントはイーサネット・コネクション・ブレードとセキュリティが確立された暗号化接続ができる。 この接続はインバウンドtelnet接続と同じ機能がある。 SSHはイーサ ネット・コネクション・ブレードの接続と認証にRSA公開鍵暗号法を使用する。

ポートによる認証**(802.1x)**

ポートによる認証で外部サーバを介してポート毎にシステム・ユーザーを認証できる。認証され許可されたシステム・ユーザーのみデータの送受信をできる。 ポートは拡張認証プロトコル (EAP)を使用するr遠隔認証ダイアルインユーザー・サービス(RADIUS) サーバを介して認証される。

RADIUSクライアント

RADIUSはクライアント/サーバ・ベースのプロトコルである。RADIUSサーバはユーザー名、パスワード、アカウント情報等ユーザー毎の認証情報を含むユーザー・データベースを維持する。詳細は"RADIUSのグローバル・パラメータを構成する"を参照のこと。

TACACS+ クライアント

TACACS+はイーサネット・コネクション・ブレードにアクセスするユーザーの認証に中央統合セキュリティ機能を提供する。TACACS+はRADIUSおよびその他の認証プロセスとの一貫性を保持しつつも中央統合型ユーザー管理システムとなる。

LDAP クライアント

Lightweight Directory Access ProtocolすなわちLDAPはTCP/IPによるサービスのクエリーと変更に用いるアプリケーション・プロトコルである。ディレクトリは同類の属性があるオブジェクトの集合を論理的で階層的に整理したものである。

サービス妨害攻撃対策

サービス妨害攻撃はコンピュータのリソースを本来のユーザーに利用できなくしようとする試みをいう。 ここでは、イーサネット・コネクション・ブレードは拡張対策機能を用いて本来のユーザーがそのリソースを利用できなくならないようにしている。

MAC Address Authentication (MAC Address Filter)

ポート·ロックは特定MACアドレスのユーザーのみにアクセスを特定のポートに限定するためネットワーク·セキュリティを強化する。 当該アドレスは手動定義によるか適用ポートで学習される。 フレームがロックされたポートで発見され、フレーム·ソースMACアドレスがそのポートには関連付けられていないと、保護機能が発動される。

IP Address Authentication (IP Address Filter)

管理IPアドレス·フィルターはイーサネット·コネクション·ブレードの構成変更を許可されるステーションを指定する。5 台までの管理ステーションをイーサネット·コネクション·ブレード管理用に選択できる。1 台以上の管理ステーションを定義しようとすると、IPアドレスにより定義された指定選択ステーションのみウェブ·マネージャ、Telnetセッション、セキュア·シェル (SSH)またはセキュア·ソケット·レイヤー (SSL)でHTTPSの管理特権を許可される。

2.1.6 QOS機能

PRIMERGY BX900 はDSCP(Differentiated Services･コード･ポイント)のCOSキューへのマッ ピングをサポートする。従って異なるDSCP値をもつパケットは異なるサービス用の別のCOSキューにスケジュール化できる。 DSCPの定義はTOS定義に下位互換性がある。 PRIMERGY BX900 はこのためTOSからCOSキューへのマッピングもサポートする。優先度が異なるパケットは異なるプライオリティのCOSキューにスケジュール化できる。

802.1pによるCoS

フレームを受信すると、イーサネット･コネクション･ブレードは 802.1Qに定義されたVLAN IDにあるプライオリティ 3 ビットを検査してそのフレームのプライオリティを決定する。フレームのプライオリティがわかると、そのプライオリティをフレームが転送されるべき各出力ポートで 4 つの出力キューのうち 1 個に利用できるよう対応づける。プライオリティ･マッピングと出力キューはWEB、CLI、またはSNMPインターフェイスを用いて自分で変更できることに注意されたい。出力キューにあるフレームは次にスケジュール化アルゴリズムに従い転送される。

IP TOS/プレシデンス/DSCPベースのCoS

フレームを受信すると、イーサネット･コネクション･ブレードはパケットのIP TOS、IPプレシデ ンス、またはDSCPが所定値と一致するかを判断する。一致した場合、このフレームのクラスと関連付けられたポリシーを照合する。ポリシーはユーザーが構成できる：DSCPフィールドを送信、破棄、マークする、プレシデンス･フィールドをマークする、またはこのクラスのフレームに特定の帯域を専用に割当てる。

アクセス･コントロール･リスト(ACL)

パケット･フィルタリングはネットワーク･トラフィックや特定のユーザーまたはデバイスによるネットワーク使用を制限できる。ACLはスイッチを通過して特定のインターファイスやVLANを横断するパケットを許可または破棄しながらトラフィックをフィルターします。ACLはパケットに適用される許可と破棄の条件を順次的に集めたものです。パケットがあるインターフェイスで受信されるとき、スイッチはアクセスリストで特定された判定基準に基づいてそのパケットが転送されるために要求される許可を得ているか照合すべく任意の適用されたACLに対するパケットの欄を比較します。スイッチは最初の一致の後テストを中止するのでリストにある条件の順序は決定的に重要です。1 つも条件が一致しなければ、スイッチはパケットを破棄します。制限がなければ、スイッチはパケットを転送します。 スイッチはパケットを中断します。スイッチは、VLAN内にブリッジされたパケットも含めそれが転送するすべてのパケットにACLを使うことができます。

これらのアクセス･リストはレイヤー2 インターフェイスでサポートされる：ソース･アドレスを使用する標準IPアクセス･リストとソース･アドレスとターゲット･アドレスおよびオプションのプロトコル･タイプ情報を使用する拡張IPアクセス･リストである。スイッチは任意のインターフェイス上に設定されたすべての受信された機能に関連したACLを照合してそのパケットがいかにACLのエントリに一致するかに基づきパケットが転送のを許可または拒絶します。こんな風に、ACLはネットワークやネットワークの一部へのアクセスを制御するために使われます。

ACLは許可と拒絶の条件を順次的に集めたものです。スイッチはアクセスリストの条件に対するパケットをテストします。最初の一致がスイッチがパケットを受け入れるか拒否するかを決定します。スイッチは最初の一致の後テストを中止しますから、条件の順序が非常に大事です。一致する条件がなければ、スイッチはパケットを破棄します。

PRIMERGY BX900 は次の種類のACLまたはIPアクセス･リストをサポートする：

- 標準IPアクセス･リストは照合に送信元･アドレスを使用する拡張IPアクセス･リストは照合に送信元･アドレスと送信先･アドレスを使用し、より粒度の高い制御にはさらにオプションのプロトコル･タイプ情報を使用する。

標準ACLは最も初期のACLである。標準ACLはIPパケットの送信元･アドレスをACLに構成されたアドレスと比較してトラフィックを制御する。標準ACLはIPパケットの送信元･アドレスと送信先･アドレスをACLに構成されたアドレスと比較してトラフィックを制御する。規則はパケットの 6 個のフィールドまで検査するように構成できる：送信元IP、送信先IP、送信元L4 ポート、送信先L4 ポート、TOSバイト、プロトコル番号。

プライオリティ・キューの厳密なスケジュール化

WRRに加え、PRIMERGY BX900 は厳密なスケジュール化もサポートし、プライオリティ・パケ ットが他のす べてのトラフィックに先んじて常に最初にサービスを受けること、他 の 3 つの キューはWRRスケジュール化によりサービスを受けることを確保している。

WRR (荷重ラウンドロビン)

PRIMERGY BX900WRRは荷重ラウンドロビン (WRR)によるスケジュール化をサポートする。 WRR キューイング・アルゴリズムではプライオリティの低いパケットが帯域を全く割当てられないことがないように、ネットワーク管理者により管理されるプライオリティ設定に影響を与えることなくサービスを受けることができる。

差別化サービス

ネットワークリソースはトラフィック分類とプライオリティにより分割され、ネットワーク管理ポリシーに従い厳格なタイミングニーズのあるデータ処理を優先的に行う。 PRIMERGY BX900 は差 別化サービス(DiffServ)をサポートする。
DiffServはリソースリザーブプロトコルを必要とせずにネットワーク・トラフィックにQoS処理を提供する方法である。具体的には管理はネットワーク機器に次の内容を識別化するようプロビジョンを行う：ネットワークにおけるトラフィックのクラスおよびトラフィック・クラスが受けるQoS処理である。

DiffServはDiffServドメインを一貫してトラフィックを許容するか、DiffServドメインを一環してトラフィックを伝送するか、さらにネットワーク・ノード内で帯域を保証するかを制御する。許容、伝送および帯域の制御により、ポリシーによるサービスの範囲が定められる。

DiffServを構成するには 3 個のキーQoS構築ブロックがある。 クラス、ポリシー、サービスである。

- Class,
- Policy,
- Services.

クラスの構成では、特定トラフィック・クラスの一致基準をユーザーが指定する。 イーサネット・コネクション・ブレードに提供される基準には次がある：

- Destination MAC address,
- Destination IP address,
- Destination layer 4 port,
- IP DSCP,
- IP Precedence,
- IP TOS,
- Protocol,
- Source MAC address,
- Source IP address,
- Source layer 4 port,
- Any

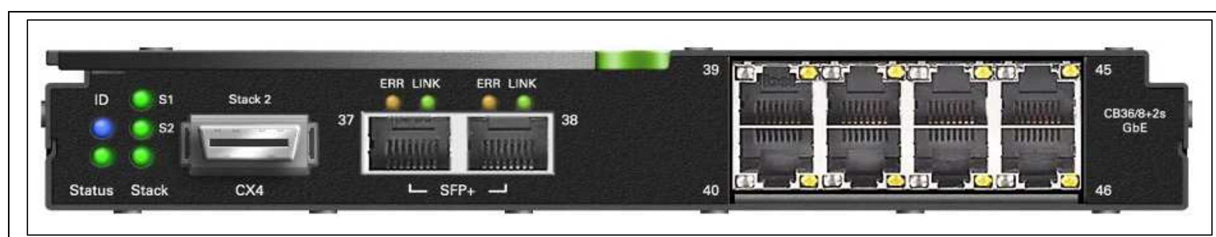
2.2 ハードウェアの説明

2.2.1 イーサネット･コネクション･ブレードのポート構成

PRIMERGY BX900 イーサネット･コネクション･ブレードには次のものが含まれます;a) PG-SW111 の場合、ネットワークに接続するための 1 ギガビットのイーサネットポートと 2 つの 10G SFP+イー サネットポート、そして 1 つのCX4 HiGig/HiGig+ポートとスタッキング目的のひとつの外部CX4 HiGig/HiGig+ポ ート、 b) PG-SW112 の場合、8 つのRJ45 ギガビット･イーサネットポートとネットワークに 接続する 4 つの SFPギガビットイーサネットポート、それは PRIMERGYBX900 ブレードサーバの管理MMBモジュールに接続するためのバンド外管理のイーサネットポートを持っています。

PG-SW111 用の物理ポート

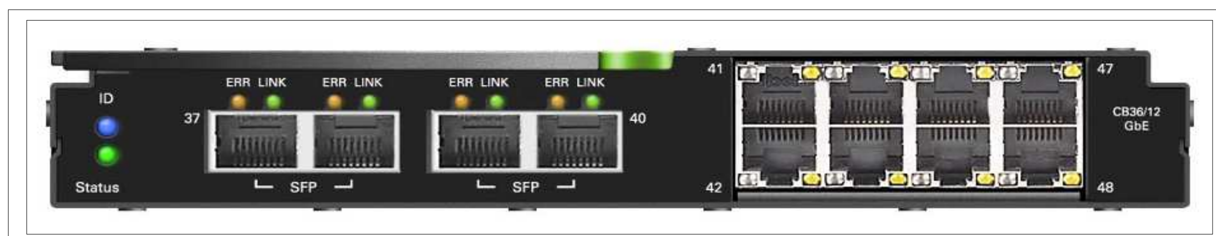
- **36 個の 1 ギガビット･ダウンリンク･ポート**
- **8 個のアップリンク･ポート用 1 ギガビットRJ45 ポート**
- **2 個のアップリンク用 10 ギガビットSFP+ポート**
- **最大 8 個のデバイスまでスタック可能な 2 個のHiGig/HiGig+ポート。 このうち 1 個はシステム中央部の内部スタック用であり、もう 1 個は外部スタック用である。**



図： PRIMERGY BX900 GbEコネクション･ブレードの 36/8+2 スタック (PG-SW111) 前面

PG-SW112 用の物理ポート

- **36 個の 1 ギガビット･ダウンリンク･ポート**
- **8 個のアップリンク･ポート用 1 ギガビットRJ45 ポート**
- **4 個のアップリンク用 1 ギガビットSFPポート**



図： PRIMERGY BX900 GbEコネクション･ブレードの 36/12 スタック (PG-SW112) 前面

8 個のRF45 ギガビット･イーサネット･ポートは 10、100、または 1000 Mbpsで動作できる。 これら のポートはネゴシエーション、二重モード(半二重または全二重)、およびフロー制御をサポートする。 サーバに接続する 36 個のダウンリンク用 1 ギガビット･イーサネット･ポートは 1000Mbps、全二重、フロー制御のみで動作可能である。

2.2.2　　イーサネット･ポート

アップリンク･ポート

8 個の外部RJ45 ポートはIEEE 802.3x自動ネゴシエーションによる速度、二重モード、 フロー 制御 を サポートする。ポートは 10Mbps、100Mbps、または 1000Mbps、半二重、全二重で動作し、 データ の流れを制御してバッファーをオーバーフローさせない。アップリンクポートは、カテゴリー5 のツイストペアのケーブルにより 100m(328 フィート)までの距離にある他のIEEE 802.3ab 100BASE-Tに準拠したデバ イスに接続できます。これらのポートはユーザーがすべての接続のために一直線状のケー ブルを使うことが できるように自動のMDI/MDI-Xの運用を特徴としています。それに加えて、PG-SW112 にあるSFPポートは単一 と二重のモードをサポートし、PG-SW111 の 10Gのポートは標準的なSFP+準拠のものです。

注 - 自動ネゴシエーションを使用する際は、速度、伝送モード、フロー制御はこの機能が接続デ バイスでもサポートされる場合自動的に設定される。これ以外の場合各項目を接続毎に手動で構成できる。

注 – 自動MDI/MDI-Xピンアウト構成のために有効化されなければならない。

内部ポート

イーサネット･コネクション･ブレードはシャーシのサーバブレードに接続する 36 個の内部 1000BASE-Xイーサネット･ポートも含む。 これらのポートは 1000Mbps、全二重に固定されている。

2.2.3 LEDの状態

フロント･パネルには発行ダイオード (LED)があり、リンク、イーサネット･コネクション･ブレード診断の状態を示す。

ポートLED

アップリンク毎に 2 個のLEDインジケータがある。

RJ45:

LED	色	意味
LED-A (速度)	オレンジ	ポート･リンク速度 1000Mbps
	緑	ポート･リンク速度 100 Mbps
	消灯	ポート･リンク速度 10 Mbps
LED-B (リンク/動作)	緑	ネットワーク･リンク
	緑点滅	ネットワーク動作中
	消灯	ネットワーク･リンクが無いまたはポートが無効

SFP:

LED	色	意味
リンク	消灯	ネットワーク･リンクが無いまたはポートが無効
	緑	SFPトランシーバ･リンクの状態
	緑点滅	SFPトランシーバ アクティブ状態
ERR	消灯	SFPエラー無し
	オレンジ	SFPトランシーバ エラー
	オレンジ点滅	SFPモジュールがサポートされていない

SFP+:

LED	色	意味
リンク	消灯	ネットワーク･リンクが無いまたはポートが無効
	緑	SFP＋トランシーバ･リンクの状態
	緑点滅	SFP＋トランシーバ アクティブ状態
ERR	消灯	SFP＋エラー無し
	オレンジ	SFP＋トランシーバ エラー
	点滅オレンジ	SFP＋モジュールがサポートされていない

汎用LED

1 個のイーサネット･コネクション･ブレード･システムLEDがあり二つの機能があり、MMBによりエラー･ｽﾃｰﾀｽ通知とブレードﾞ識別を制御される。 異なる点滅周波数が使用され異なる機能を示す。 識別とエラー通知の二機能があり、エラー通知より識別が優先される。

LED	色	意味
ID	青	コネクション･ブレードを識別する
	消灯	通常
状態	緑	電源投入状態
	点滅オレンジ	コネクション･ブレードの障害
	消灯	電源遮断状態
S1	緑	内部スタック･ポート 1 のリンク
	緑点滅	内部スタック･ポート 1 の動作
	消灯	スタック･ポート 1 のリンク無し
S2	緑	外部スタック･ポート 2 のリンク
	緑点滅	外部スタック･ポート 2 の動作
	消灯	スタック･ポート 2 のリンク無し
スタック	黄	コネクション･ブレードはスタック･マスター
	黄点滅	コネクション･ブレードがマスター機能を果たせない
	緑	コネクション･ブレードはスタック･スレーブ
	緑点滅	マスター選択中
	消灯	コネクション･ブレードがスタックに無い

2.2.4 サポートされるSFP+とSFPのベンダー一覧表

サポートされるSFPモジュール:

ベンダー	製造番号P/N
フィニサー社	FCLF-8521-3
フィニサー社	FTLF8524P2BNV

サポートされるSFP + モジュール:

ベンダー	製造番号P/N
オプネクスト社	TRS2000EN-S002
フィニサー社	FTLX8571D3BCL

2.3 機能と利点

2.3.1 接続機能

- 36 個の内部ギガビット・ポートでサーバ・カードの容易なネットワークへの統合が可能。
- 8 個の外部 1000BASE-Tギガビット・ポートが業務ネットワークへのアップリンクを提供。
- 4 個のSFPギガビット・ポートが業務ネットワークへのアップリンクを提供。 (PG-SW112)
- 2 個のSFP＋ 10 ギガビット・ポートが業務ネットワークへのアップリンクを提供。 (PG-SW111)
- 外部ポートの自動MDI/MDI-Xサポートによりすべての接続をストレート・ケーブル (自動ネゴシエーションが有効化された状態で) でも可能。
- 自動ネゴシエーションはポート毎に最適速度 (10、100、または 1000Mbps)と通信モード (半二重か全二重) の自動選択を可能にする。ただし接続機器にこの機能がある場合。これ以外の場合、ポートは手動構成できる。
- IEEE 802.3adギガビット・イーサネット準拠によりベンダーの規格準拠ネットワーク・カードとスイッチと互換性が保たれる。

2.3.2 性能

- トランスペアレントブリッジング転送モード： 保存-転送
- 帯域： 152Gbps (PG-SW111) / 96Gbps (PG-SW112)
- スイッチング遅延： 64 バイト・フレームでは平均 8us
- スイッチング・テーブル、8K (PG-SW112) /16K (PG-SW111) MAC アドレス・エントリ
- 平均故障間隔 (MTBF): 175699 時間

2.3.3 管理

- Telnet、SNMP/RMON、ウェブ・ベースのインターフェイス
- 高速なポートの再構成をした(たとえば高速転送セットアップ)、冗長なネットワーク接続のためのスパニングツリープロトコル
- 4 本の別個キューでサポートされるQoS
- IGMP(インターネット・グループ管理プロトコル) /MLDスヌーピングによるフィルタリングに基づくマルチキャスト・スイッチング
- ブロードキャスト・ストーム抑制
- ポート・ミラーリング
- リンクアグリゲーション
- ユーザー名とパスワード、SNMPコミュニティー名による管理アクセス・セキュリティ

2.4 表記規則

この手順書で使用される記号やフォントの意味を次に定義する。

⚠ 要注意	この記号を付された文には特に注意を払うこと。 この警告に従わないと人命への危険、システムの破壊、データ損失に至るおそれがある。
引用符””	章の名前、強調される用語に使う。
i 注意:	この記号は補足的情報、備考、ヒントとともに用いられる。

2.5 この手順書の対象ユーザー

この手順書はネットワーク接続の設置と構成を担当する技術要員を対象とする。 この手順書にはイーサネット・コネクション・ブレードを構成するために必要な情報がすべて掲載される。

2.6 テクニカル·データ

電気系データ

運転電圧	+12 VDC @ 2.5 A 最大 (PG-SW112) +12 VDC @ 3.5 A 最大 (PG-SW111)
最大電流	7.52 A max @ 3.3 VDC 11.8 A max @ 2.5 VDC 24 A max @ 1.25 VDC 7.76 A max @ 1 VDC

国内および国際規格

製品の安全性	IEC 60950 / EN 60950 / UL 60950, CSA 22.2 No. 950
電磁両立性 干渉エミッション 高調波電流 フリッカー 干渉耐性	FCC クラスA VCCI クラスA AS / NZS 3548 クラスA EN 55022 EN 61000-3-2 JEIDA EN 61000-3-3 EN 55024 EN 61000-4-2/3/4/5/6/8/11 BSMI CNS 13438
EU指令によるCE認証:	73/23/EEC (低電圧指令) 89/336/EEC (電磁両立性)

寸法

長さ (L)	276.24 mm
幅 (W)	192.63 mm
高さ (H)	28.04 mm

環境条件

環境クラス 3K2 環境クラス 2K2	DIN IEC 721 パート 3-3 DIN IEC 721 パート 3-2
温度: – 稼働時 (3K2) – 輸送中 (2K2)	 0 ° C .... 50 °C -40 °C .... 70 °C
湿度	10 ... 90%

稼動中の結露は必ず回避すること。

3 ネットワーク計画

3.1 スイッチングの紹介

ネットワークのスイッチはノン・クロスバーのスイッチングによって多重のパケットを同時に送信することを可能にする。このことはそれがブリッジやルータよりも効率的にネットワークをパーティションできることを意味する。したがってスイッチは今日のネットワーク技術にとて最も重要な基礎的要素の一つと認識されています。

ネットワークアクセスポイントでの輻輳で(例えば、高容量のファイルサーバのネットワークカード)性能の障害が引き起こされたとき、輻輳するデバイスを(例えばサーバまたユーザー)スイッチポートに直接設定することができます。これはイーサネットセグメントの最大限のバンド幅をスイッチ上の単一のポートに付いたデバイスへ割当てます。そして完全なデュプレックスを稼働するとき、専用のセグメントのバンド幅を 2 倍にしてさらにスループットを最大化できます。

ネットワークがリピーター(ハブ)技術に基づくなら、ステーション間の最大限の距離は限られています。 従来のイーサネットなら、1 組のステーション間には 4 つまでのハブがあるでしょう。」高速イーサネットならば最大限 2 つです。これはホップカウントとして知られています。しかしながらスイッチはホップカウントをゼロに戻し、ネットワークを再分割してより小さな管理しやすいセグメントにし、そしてスイッチを用いてそれらをリンクさせ大きなネットワークを作り、その結果この制限を取り除きます。

イーサネット・コネクション・ブレードは旧来のケーブル敷設とネットワークカードを使いながらバンド幅を著しく引き上げるためのイーサネットネットワークへと容易に構成することができる。

3.2 用途例

イーサネット・コネクション・ブレードはネットワークを統合するよう設計されており、ネットワーク・コアはサーバシャーシとワークグループ・スイッチの間に広帯域接続を提供できる。 この節でその一部の主要用途を説明する。

3.2.1 バックボーン接続

スイッチは高速ギガビット・イーサネットリンクを使ったネットワークのバックボーンや他のキーサイトへ接続でき、そして全体のバンド幅とスループットを増やします。

下の図で、アップリンク・ポートは 2 Gbpsの完全デュプレックス接続を企業のバックボーンへ、インター ネットへ、そして他のサーバへ供給しています。

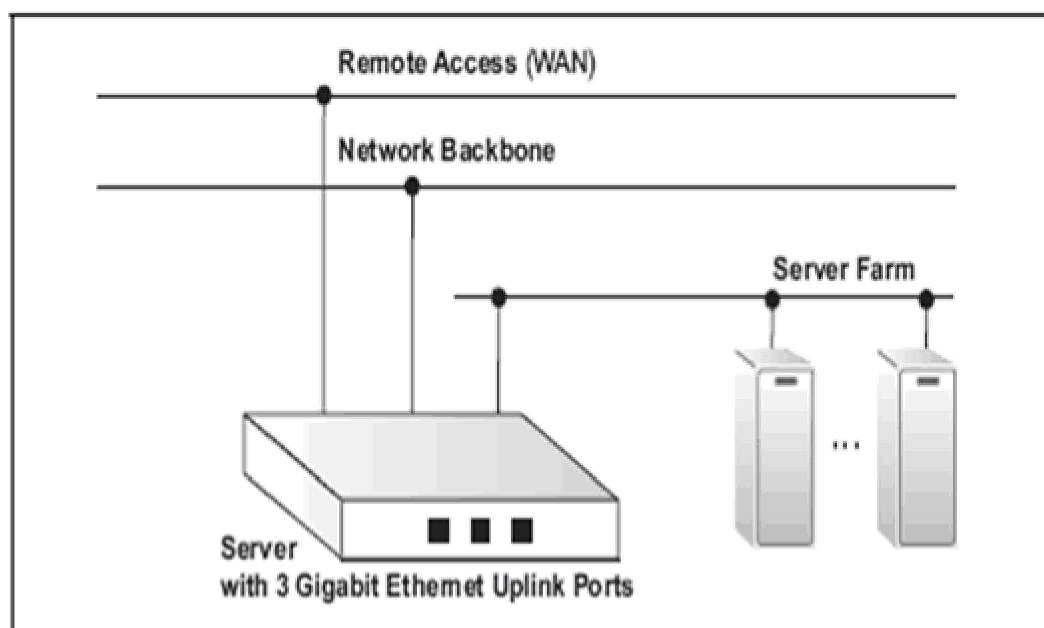


図:バックボーン接続

3.2.2 VLAN接続を作る

スイッチは任意のネットワーク・ノードのグループを編成して別々のブロードキャスト・ドメインを作るために使うことのできる仮想LAN (VLAN)をサポートします。VLANはブロードキャスティングのトラフィックを始発グループに限定し、大きなネットワークでのブロードキャスト・ストームを解消できます。これはより安全で欠点の少ないネットワーク環境を提供します。

VLANはタグの付かないポートグループを基に設計できるか、あるいはトラフィックはそれが属するVLANのグループを識別するためにタグが付けられます。タグ無しのVLANは単一のスイッチに付けられた小さなネットワーク用に使われます。しかし、タグ付きのVLANは大きなネットワークに使われます。すべてのVLANにはスイッチ相互間のリンクが割当てられます。

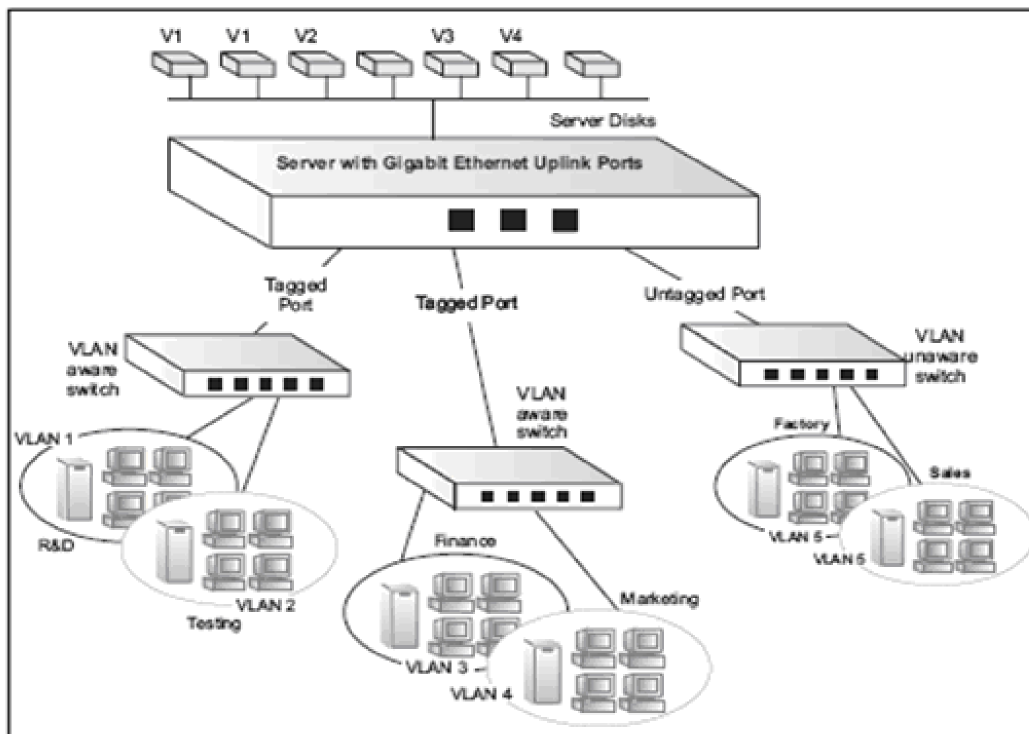


図: VLAN接続を作る

スイッチまたはUEEE 802.1Qタグをサポートしない他のネットワークデバイスへ接続するときは、タグ無しのポートによりください。

4　ネットワーク接続を確立する

イーサネット・コネクション・ブレードはシステム内に取付けられたサーバボードを共通スイッチ・ファブリックに接続するとともに、外部ポートをIEEE 802.3ab準拠の外部機器にアップリンクする ように提供する。ほとんどの用途ではイーサネット・コネクション・ブレードの外部ポートはネットワーク・バックボーンにある他のスイッチに接続することができる。さらにPCやサーバのギガビット・イーサネット・ネットワークにも直接接続できる。



ケーブルに接続する前に、ネットワークループを避けるため、スパニングツリープロトコルを先ず構成したほうがよいです。詳細は「スパニング・ツリー・プロトコルの構成」のセクションを参照してください。

4.1　1000BASE-T機器に接続する

スイッチのこのデータポートはシード、二重モードとフロー制御の自動ネゴシエーションをサポートし、10Mbps、100Mbps、1000Mbps半二重と全二重が可能である。1000BASE-T規格は最大長 100m(328 フィート) までの接続に Cat5 ツイストペア・ケーブルを 4 対使用する。



1000Mbps接続ではケーブルがIEEE 802.3ab 1000BASE-Tに準拠して設置できる か試験する必要がある。 詳細は"1000BASE-Tケーブル要件"を参照されたい。

1. ネットワークを構成する機器の準備をする。1000Mbps 接続には、サーバとワークステーションに 1000BASE-T ネットワーク・インターフェイス・カードが取付けられていることを確認すること。 他のネットワーク機器は IEEE 802.3ab 1000BASE-T 規格に準拠する RJ45 ポートがなければ ならない。
2. RJ45 プラグが両端にあるシールドまたは非シールド・ツイストペア・ケーブル (ストレートまたはクロスオーバー) を準備する。1000Mbps ギガビット・イーサネット接続用の 100Ω Cat5 (Cat5e 以上を推奨)ケーブルを使用すること。
3. ケーブルの片方の先端を別のデバイスの RJ-45 ポートに接続し、他方の端をスイッチにある任意の RJ-45 ポートに接続します。RJ45 プラグを差し込む際、プラグにあるタブがカチッとはまり、正しく 固定されることを確認する。



RF45 ポートに電話用ジャックコネクタを差し込まないこと。イーサネット・コネクション・ブレードを損傷することがある。必ず、FCC規格準拠のRJ45 コネクタ付きツイストペア・ケーブルのみ使用する。



1000Mbps接続にはケーブルの 4 対すべてを接続しなければならない。自動ネゴシエーションが有効化されている場合、1000BASE-Tポートは自動MDI/MDI-X 機能をサポートする、 すなわちストレート機器であっても 10Mbps、100Mbps、または 1000Mbpsの速度をサポートできる。 ツイストペア・ケーブル 1 本は 100m(328 フィート) を超えないようにする。 自動ネゴシエーションは自動MDI/MDI-Xのサポートには有効化されなければならない。

4.2 1000BASE-Tケーブル要件

100BASE-TXで使用するすべてのCat5UTPケーブルなら 4 対ラインすべて が接続されていれば 1000BASE-Tにも使用できる。しかしすべての基幹接続または新たなケーブルの 設置の場合、 Cat5e (拡張Cat5)ケーブルを使うこと。Cat5e規格はCat5 のみに推奨されるテスト・パラメータを含む。従って、1000BAST-Tを実行するために既存Cat5 ケーブルを準備する 際最初に行う べきことは、IEEE 802.3ab規格準拠性を確かめるために、 設置されたケーブルを単にテストする。

4.2.1 既存Cat5 ケーブルのケーブル・テスト

敷設済みのCat5 ケーブルは減衰、近端漏話(NEXT)、遠端漏話(FEXT)のテストに合格しなければならない。 このケーブルテスト情報はANSI/TIA/EIA-TSB-67 規格に指定されている。 さらに、反射損失と 等レベル遠端漏和(ELFEXT)のテスト・パラメータにも合格しなければならない。これらのテストは ANSI/TIA/EIA-TSB-95 冊子”100Ω4 対Cat5ケーブルの追加的伝送性能ガイドライン"に指定 されている。

設置されたケーブルを検査するには、必ずスイッチと末端デバイスの間のすべてのパッチを含めてください。

4.2.2 既存Cat5 ケーブルを 1000BASE-Tに調整する

既存のCat5 敷設ケーブルが 1000BASE-Tのテスト・パラメータの一つに不合格な場合、問題を修正する ために 適用できる 3 つの基本措置がある。

1. Cat5 パッチケーブルを高性能 Cat5e ケーブルと交換する。
2. リンクに使用されるコネクタ数を減らす。
3. リンクのコネクタの一部を抜いてから再び接続してみる。

4.2.3 1000BASE-Tのピン割当て

1000BAST-Tポートは自動MDI/MDI-Xをサポートするので、PCやサーバまたは他のスイッチとの すべてのネットワーク接続にストレート・ケーブルを使用できる。 (自動ネゴシエーションはMDI/MDI-Xをサポートするには有効化されなければならない。)

次表は 1000BASE-T MDIとMDI-Xポートのピン配列を示す。

これらのポートではワイヤの 4 対すべてが接続されることが要件である。1000Mbps接続ではワイヤの 4 対すべてが送受信の両方に使用されることに注意する。

1000Mbps接続には 100ΩCat5 かCat5eの非シールド・ツイストペア (UTP)またはシールド・ツイストペア(STP) ケーブルを使用する。ツイストペア接続の長さが 100m(328 フィート)を超えないようにする。

Pin	MDI Signal Name	MDI-X Signal Name
1	Transmit Data plus (TD1+)	Transmit Data plus (TD2 +)
2	Receive Data minus (RD1-)	Receive Data minus (RD2-)
3	Transmit Data plus (TD2+)	Transmit Data plus (TD1+)
4	Transmit Data plus (TD3+)	Transmit Data plus (TD4+)
5	Receive Data minus (RD3-)	Receive Data minus (RD4-)
6	Receive Data minus (RD2-)	Receive Data minus (RD1-)
7	Transmit Data plus (TD4+)	Transmit Data plus (TD3+)
8	Receive Data minus (RD4-)	Receive Data minus (RD3-)

Pin	MDI Signal Name	MDI-X Signal Name
1	Transmit Data plus (TD1+)	Transmit Data plus (TD2 +)
2	Receive Data minus (RD1-)	Receive Data minus (RD2-)
3	Transmit Data plus (TD2+)	Transmit Data plus (TD1+)
4	Transmit Data plus (TD3+)	Transmit Data plus (TD4+)
5	Receive Data minus (RD3-)	Receive Data minus (RD4-)
6	Receive Data minus (RD2-)	Receive Data minus (RD1-)
7	Transmit Data plus (TD4+)	Transmit Data plus (TD3+)
8	Receive Data minus (RD4-)	Receive Data minus (RD3-)

表; 1000BASE-Tのピン配列

5　　イーサネット･コネクション･ブレードを構成する

この節はイーサネット･コネクション･ブレードの開梱、設置、ケーブル接続について説明する。

5.1　　概　要

イーサネット･コネクション･ブレードはPRIMERGY BX900 ブレードサーバに挿入され、プ ロセ ッサ･ブレードは 18 枚までイーサネット･コネクション･ブレードは 8 台まで統合できるサーバモジュールである。

梱包の内容

イーサネット･コネクション･ブレードを開梱する際、次の品目が含まれていることを確認する。

- イーサネット･コネクション･ブレード

イーサネット･コネクション･ブレードの開梱

イーサネット･コネクション･ブレードを開梱する手順:



イーサネット･コネクション･ブレードを開梱する前に、梱包内容を検査して損傷が明らかにあれば直ちに報告する。

静電で損傷しやすいデバイス用ストラップは同梱されてはいないが、次から先の手順を行う際はストラップを着用したほうがよい。

1. 容器を開く。
2. イーサネット･コネクション･ブレードを容器から注意して取り出し、安全で清潔な表面に置く。
3. 梱包資材をすべて取り去る。
4. イーサネット･コネクション･ブレードに損傷がないか点検する。 損傷があれば直ちに報告する。



この資料の図解は実物イーサネット･コネクション･ブレードとシャーシとは若干異なる場合がある。

5.2 イーサネット･コネクション･ブレードを接続する

イーサネット･コネクション･ブレードを構成する前に、PRIMERGY BX900 ブレード･サーバの コンソール･ポートをイーサネット･コネクション･ブレードに接続しなければならない。 PRIMERGY BX900 ブレード･サーバのコンソール･ポートをイーサネット･コネクション･ ブレードに接続する手順は以下の通りである:

1. イーサネット･コネクション･ブレードを取付ける

コンソール･モニターに MMB アプリケーションのログイン画面が表示される。

イーサネット･コネクション･ブレードの起動画面が表示される。

```
                    Welcome to Management Blade 1.30J


<Username>:
```

2. 支給されたユーザー名とパスワードを入力する。 コンソール･メニューが表示される。

```
                    Welcome to Management Blade 1.30J


<Username>:admin
<Password>:*****

+---------------------------------------------------------------------------+
|                      Console Menu                    page_root
+---------------------------------------------------------------------------+
(1) Management Agent
(2) Emergency Management Port
(3) Console Redirection
(4) TFTP update
(5) Logout
(6) Reboot Management Blade
(7) System Information Dump
(8) Command Line Interface
(9) Account Management
Enter selection: 3
```

3. (3) Console Redirection を選択する。 Console RedirectionTable （コンソール･リダイレクション･テーブル） が表示される。

```
+---------------------------------------------------------------------------+
|           Console Redirection Table                                page_3
+---------------------------------------------------------------------------+
(1) Console Redirect Connection Blade
(2) Set Return Hotkey , Ctrl+(a character) : Q
(3) Set Console Redirection Timeout          : 900
Enter selection or type (0) to quit: 1
```

4. (1) Console Redirection Connection Blade を選択する。 Console Redirect Connection Blade が表示される。

```
+---------------------------------------------------------------------------+
|           Console Redirect Connection Blade                        page_3_1
+---------------------------------------------------------------------------+
(1) Console Redirect Connection Blade-1
(2) Console Redirect Connection Blade-2
Enter selection or type (0) to quit: 1
```

5. リダイレクトするコネクション･ブレードを選択する。 次にEnterを押してコンソールがリダイレクトされたかを確認する。

```
Press <Ctrl+Q> Return Console Menu


(BX900-CB1)#
```

5.3 イーサネット·コネクション·ブレードの起動と構成

イーサネット·コネクション·ブレードを構成する際イーサネット·コネクション·ブレードのアーキテクチャを理解しておくことが重要である。イーサネット·コネクション·ブレードには 2 種類のポートがある。 一つはイーサネット·コネクション·ブレードとPRIMERGY BX900 ブレード·サーバ とのインターフェイス用、もう一つはPRIMERGY BX900 ブレード·サーバを外部ネット ワークに接続するための普通のイーサネット·ポートである。

PRIMERGY BX900 ブレード·サーバはPRIMERGY BX900 ブレード·サーバの (管理ボード) MMB とは内部ポートと呼ばれる 36 個の内部ポートにより接続される。内部ポートのリンク最高速度はポート毎に 1 ギガビットである。ポート構成IDは 1 から 36 までである。イーサネット·コネクション·ブレードを外部ネットワークと接続するために、外部ポートと呼ばれる、8 個のPHYベース·ポート、4 個の 1 ギガビットSFPポートまたは 2 個のSFP+10 ギガビット·ポート (プラットフォーム·タイプにより異なる)がある。

内部ポートと外部ポートのデフォルト構成は次の通りである：

外部ポート	
意味	**初期設定**
フロー制御	オフ (入口では無効化されている)
バック·プレッシャ	オフ (入口では無効化されている)
自動ネゴシエーション	有効

表; 外部ポートのデフォルト構成

内部ポート	
意味	**初期設定**
速度と二重自動ネゴシエーション	1 ギガビット フルスピード
フロー制御	無効
フロー制御の自動ネゴシエーション	無効

表;外部ポートのデフォルト構成

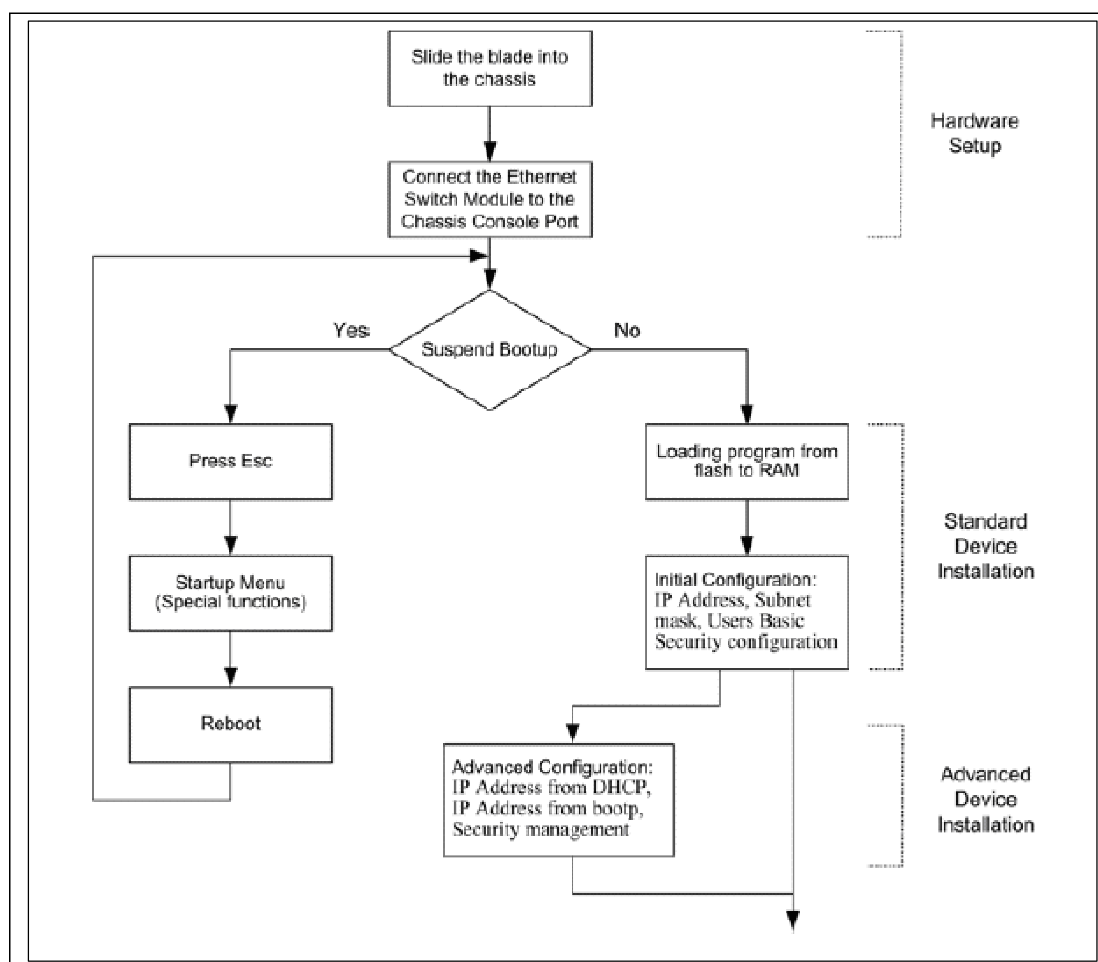


図: 設置と構成作業の流れ

5.4 端末を構成する

デバイスを構成するには、ステーションは端末エミュレーション・ソフトウェアを実行していなければならない。イーサネット・コネクション・ブレードが正しく取付けられ、シャーシのシリアルポートに接続されていることを確認する。 端末エミュレーション・ソフトウェアは次のように設定する: PRIMERGY BX900 マネジメント・ブレードのシリアルポートに接続し、コンソール・ リダイ レク ト 機能を使用してイーサネット・コネクション・ブレードにコンソールからアクセスできるようにする。



1. データ形式をボーレート 115200、データビット 8、ストップビット 1、パリティ無しに設定する。
2. フロー制御を無しに設定する。
3. プロパティで、エミュレーション・モードのために VT100 を選択する。
4. 機能、矢印、Ctrl キーに端末キーを選択する。 この設定は端末キー用である (ウィンドウズキーとは異なる) 。

端末からイーサネット・コネクション・ブレードにアクセスするには次の手順を踏む:

1. 端末をマネジメント・ブレードのシリアルポートに接続する。
2. マネジメント・ブレードのコンソール・リダイレクト機能を使用して必要なイーサネット・コネクション・ブレードへのアクセスを得る。
3. 何回か<Enter>キーを押して端末接続が成功したか確認する。

5.5 デバイスを起動する

イーサネット・コネクション・ブレードがローカルのターミナルに接続されるとき、デバイスのイーサネット・コネクション・ブレードは電源投入時自己診断(POST)を受けます。電源投入時自己診断はデバイスが初期化される度に実行され、ハードウェア部品を検査してデバイスの起動が完了する前にデバイスが完全に機能するかを同定する。 重要な問題が検出されると、プログラム・フローは止まる。端末にPOSTが診断結果の 成功か失敗を表示する。

デバイスが起動すると起動時診断はまずデバイス・メモリの可用性を調べてから、起動を継続する。 次の画面はPOST表示例である。

```
------------ Performing Power-On Self Tests (POST) --------------
   System SDRAM Test..........···············.........PASS
   CPU Self Test.......................·····················.PASS
   UART Loopback Test.................················..PASS
   Flash Memory Initialize............···················.PASS
   Flash Memory Checksum Test.........··········...PASS
   PCI Bus Initialize and Test........···················PASS
   System Timer Test..................···················..PASS
   I2C Bus Initialize and Test························.PASS
   Ethernet Physical Test·····························PASS
---------------Power-On Self Test Completed---------------------------


Press [Ctrl+B] to enter back door or any key to continue···
```

起動には約 60 秒を要する。

POST終了時 (最終行を参照) に表示される自動起動メッセージは、起動中に問題が無かったことを示す。 BootROM Back Door Command Line Interface (BootROMバックドア・コマンド・ライン・イ ンターフェイス) を使用して特殊手順を実行できる。 BootROM Back Door CLIに入るには、 Ctrl+Bを自動起動メッセージ表示から 2 秒以内に押す。Ctrl+Bを押してもシステム起動が中断されない場合、RAMにロード中コードを解凍し続ける。コードはRAMから実行を開始し、番号付システム・ポート・リストとその状態 (アップリンクかダウンリンクか) が表示される。デバイスの起動が完了すると、システム・プロンプトが表示されるので、ここからデバイスを構成する。デバイスを構成する前に最新ソフトウェア・バージョンがデバイスにインストールされていることを確認する。最新バージョンでなければ、最新バージョンをダウンロードしてインストールする。最新バージョンのダウンロードについて詳細は、"ソフトウェア・ダウンロード"の節を参照のこと。

5.6 ソフトウェア･ダウンロード

5.6.1 BootROMバック･ドアCLIから

Xmodemプロトコルによるソフトウェアのダウンロード (未サポート)

ソフトウェアのダウンロード手順は最新バージョンをダウンロードして破損したファイルを交換したりシステム･ソフトウェア (システムおよび起動イメージ) を更新またはアップグレードする必要があるときに行う。

BootROM CLIからソフトウェアをダウンロードするには:

1. **BootROM CLI** プロンプトから次のコマンドを入力する: xmodem –rb <filename>
2. ハイパーターミナルを使用するときは、ハイパーターミナルのメニューバーから **Transfer** をクリックする。
3. **Filename** フィールドにダウンロードするファイルへのパスを入力する。
4. **Protocol** フィールドで Xmodem プロトコルが選択されていることを確認する。
5. **Send** をクリックする。 ソフトウェアがダウンロードされる。

デバイス構成を消去する

1. **BootROM CLI** プロンプトから次のコマンドを入力する

   delete <configuration filename>

   次のメッセージが表示される:

   Are you sure you want to delete <configuration filename> (y/n)? (<構成ファイル名>を本当に削除するか、の意)

2. **Y を押す。次のメッセージが表示される:**

   Updating partition table, please wait … Done (パーティション･テーブルの更新中、、、、完了、の意)

   Image file <configuration filename> deleted.

3. **デバイスの初期構成手順を繰り返す。**

起動イメージのダウンロード

Xmodemプロトコルを使用して新たな起動イメージをロードし、それをフラッシュメモリに書き込むと起動イメージが更新される。 起動イメージはデバイスの電源を投入するとロードされる。 ユーザーは起動イメージ･コピーを制御できない。Xmodemプロトコルで起動イメージをダウンロードするには:

1. ダウンロードするファイルを PC ホスト (イメージ･ファイル) に保存する。
2. **BootROM> dir –l** コマンドを入力して現在デバイスで実行されているソフトウェア･バージョンを確認する。 以下は表示される情報例である:

```
BootROM > dir -l
type      zip   def   date        version    name
-------------------------------------------------------------------------------
loader    none  yes   2008/12/14  0.4        PG-SW111a-l-0.4.1214.bin
bootrom   gzip  yes   2008/12/14  0.4        sb11a-b-0.4.1214.biz
runtime   gzip  yes   2008/12/10  0.5        sb11a-sw-r-0.5.1210.biz
```

```
Total: 3 files.
```

3. **BootROM CLI プロンプトから次のコマンドを入力する： xmodem –rb <filename>**
4. **ハイパーターミナルを使用するときは、ハイパーターミナルのメニューバーから Transfer をクリックする。**
5. **Filename フィールドにダウンロードするファイルへのパスを入力する。**
6. **Protocol フィールドで Xmodem プロトコルが選択されていることを確認する。**
7. **Send をクリックする。 ソフトウェアがダウンロードされる。**
8. **リセット・コマンドを入力する。 次のメッセージが表示される：**

```
BootROM> reset
Are you sure you want to reset the system (y/n)? y

System Resetting…
```

9. **Y を入力する。デバイスが再起動する。**

5.6.2 オペレーション・コードCLIによる

TFTP/FTPサーバからのソフトウェアがダウンロード

この節はTFTP/FTPサーバからデバイス・ソフトウェアをダウンロードする手順を説明する。TFTP/FTPサーバはソフトウェアをダウンロードする前に構成しなければならない。

システム・イメージのダウンロード

デバイスが起動し、システム・イメージが保存されているフラッシュメモリの領域からシステム・イメージを解凍すると実行する。新たなイメージがダウンロードされると、他のシステム・イメージ・コピーに割当てられた別の領域に保存される。次回の起動時に、デバイスは別のイメージが選択されなければ現在アクティブなシステム・イメージを解凍して実行する。

TFTP/FTPサーバからシステム・イメージをダウンロードするには：

1. IP アドレスがデバイスの 1 個のポートに構成されており、TFTP/FTP サーバに ping が送られることを確認する。
2. ダウンロードするファイルが TFTP/FTP サーバ (イメージ・ファイル) に保存されることを確認する。
3. **(CB)#show version** コマンドを入力して現在デバイスで実行中のソフトウェア・バージョンを確認する。 以下は表示される情報例である：

```
(CB) #show version
 Serial number              :SQ823LW00114
 Hardware Version           :1.0
 Number of ports            :48
 Label Revision Number     :1
 Part Number                 :A3C40096531
 Machine Model              :PY CB Eth Switch/IBP 1Gb 36/12
 Loader version             :0.7
 Operation code version     :0.40
 Boot rom version           :0.9
```

4. **(CB)#whichboot** コマンドを入力して、どのシステム・イメージが現在アクティブであるかを確認する。 以下は表示される情報例である：

```
Boot-System....................... Switch
Next Booting Mode................. Switch

                   file name              file type    startup    size (byte)
---------------------------------   -----------------------   -------   --------------
  sb11a-b-0.9.0212.biz      Boot-Rom image    Y            373327
               default.cfg      Config File            Y               19204
sb11a-sw-r-0.40.0227.biz   Operation Code     Y           8233676
```

5. **(CB)#copy tftp://{tftp address}/{file name} image {file name}**または **copy ftp://{ftp address}/{file name} image {file name}** コマンドを入力して新たなシステム・イメージをデバ イスにコピーする。次のメッセージが表示される：

```
(CB) #copy tftp://192.168.2.1/sb11a-sw-r-0.40.0227.img image sb11a-sw-r-0.04.0227.biz


Mode.......................................... TFTP
Set TFTP Server IP............................ 192.168.2.1
TFTP Path..................................... ./
TFTP Filename................................. sb11a-sw-r-0.40.0227.img
Data Type..................................... Code
Destination Filename.......................... sb11a-sw-r-0.04.0227.biz


Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n)
```

6. Y を押す。新たなイメージがダウンロードされると、他のシステム・イメージ・コピーに割当てられた別の領域に保存される。
7. **boot-system** コマンドを入力して次の起動用イメージを選択する。 このコマンドの後、**(CB)#whichboot** コマンドを入力して起動システム・コマンドでパラメータとして示されたコピーが次の起動用に選択されたことを確認する。
8. 再ロードのコマンドを入力する。 次のメッセージが表示される：

```
(CB)# reload
Are you sure you would like to reset the system? (y/n) y
```

9. Y を入力する。デバイスが再起動する。



1. システムには 2 個の実行時イメージのみ保存できる。
2. 工場デフォルトを含む 10 個までの構成ファイルがシステムに保存できます。

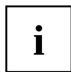
5.7 ソフトウェアの起動モードを切り替える

イーサネット・コネクション・ブレードにはスイッチ機能とIBP機能から成る 2 種類のファームウェア・バージョンがバンドルされている。 一度には 1 つのモードでのみ実行可能である。別のモードで実行 するには、起動モードを変更してイーサネット・コネクション・ブレードを再起動しなければならない。

ソフトウェア・モードを変更するには：

1. (CB)#boot-system mode コマンドを入力して次の再起動後にデバイスで実行する ソフトウェア・バージョンを指定する。
2. 次の起動時ソフトウェア・モードを IBP に変更するには、(CB)#boot-system mode IBP コマンドを使用する。
3. 次の起動時ソフトウェア・モードをスイッチに変更するには、(CB)#boot-system mode switch コマンドを使用する。

この変更はパワー・サイクルまたはソフトウェアの再起動サイクルに影響される。



コネクション・ブレードは対応して保存されたファームウェアのデフォルト起動構成により起動する、たとえば、IBP起動はibp構成により、スイッチ起動はスイッチ構成による。 これら 2 種類の構成は無関係である。

6　スタック機能を理解する

6.1　序文

スタッキング機能はHiGig/HiGig+ポートのインフィニバンドCX4 のインターフェイスを通じて接続されるスイッチのグループセットです。スタックモジュールの動作を制御するスイッチはスタック･マスターと呼ばれます。他のスイッチはスタックグループシステムのスタックメンバーに属します。

スタッキングの機能はスタックのすべてのスイッチを管理する単一点を与えることにより管理を簡素化し、ポート密度を高くします。スタック内部のスイッチはすべて 1 個のスイッチ製品として機能します。単一のIPアドレスがCLI/Web/SNMPの管理のために要求される一方、単一のコンソール/Telnetのセッションはスタックを全体管理できます。次のリストはPG-SW111 スイッチのスタッキングの利点です:

1. ネットワークで必要とされる IP アドレス数が少なくなる。
2. ネットワークは拡張されてネットワークのより広い帯域を処理できると同時に、小規模グループまたは配線の簡素化ができる
3. 高い可用性機能を提供する。1 ユニットが故障したりケーブルが偶発的に外れても、スタックの他のユニットは稼働を続けるので中断が無い。 (注 1)
4. スタックに参加する新たなユニットはスタックをリセットせずに適切に起動する(注 2) 。
5. スタックから外れるユニットはスタックをリセットせずに適切に取り除ける(注 2) 。
6. マスターの自動選択
7. 構成の自動同期化
8. スタック全体にファームウェア･アップグレードを容易に適用可能

スタッキング･ソフトウェアは各々のデバイスのテーブルを構成し、すべてのスイッチ機能をサポートするために登録します。機能とはたとえばスイッチング、リンクアグリゲーション、ポート監視、スパニングツリープロトコル、VLAN等です。全体のスタックは1個のスイッチに見えます。スタックされたシステムが正しく機能するには、個々のチップが相互に整合的にプログラムされていなければなりません。PG-SW111 デバイスがスタックへ挿入または取り出されたりするので、システムが稼働を継続できるように、チップのすべての動的再構成が必要です。これはトポロジーを発見し、監視し、スタックのチップを構成するいくつかのソフトウェアによって実現されます。

i

1. スタックはフル帯域接続により構成しなければならない (リング･トポロジー)
2. スタックの運用は、スタックマスターを削除するか電源の入ったスタンドアローンのスイッチを追加したのでない限り、メンバー登録の変更中でも中断されずに続きます。

6.2 スタック機能概要

PRIMERGY BX900 GbEコネクション·ブレードの 36/8+2 スタック(PG-SW111) は次のスタック 機能を提供する:

1. リング·トポロジーによるスタックのみ冗長構成をサポートする。 冗長構成機能はリング·トポロジーによるスタックにバックアップ·メンテナンスを保持させせなければならない。
2. スタックは最大 8 個のメンバースイッチを含む。
3. スタックは 1 個のスイッチとして管理され 1 個の IP アドレスを持つ。
4. スタックは自動的にマスタースイッチとネゴシエートする。
5. スタックマスターが利用できなくなれば、新しいスタックマスターが残っているスイッチから自動的に選ばれる。
6. 自己構成と自己管理
7. スイッチは電源の入ったスイッチを除いてスタックにある他のスイッチを中断させせることなくスタックへ追加や削除できます。
8. LAG は全体のスタックのポートで可能であり、単一のスイッチに限定されない。
9. スタック·マスターからは一意の構成入力が行われる。
10. スタック·マスターからは一意のファームウェア·アップグレードの入力が行われる。
11. マスター役は 1 つのユニットからスタック内の他のユニットに移転できる。
12. 状態 LED サポートによりどのデバイスがスタック·マスターかが示される。

6.3 スタック･マスターの選定プロセス

PG-SW111 のスタック機能は 2 個の専用 12 ギガビットHiGig+ポートにより行われる。 このうち 1 個の専用ポートは内部スタック･リンクと呼ばれる内部接続され、別の 1 個の専用ポートは外部スタック･リンクと呼ばれるフロント･パネルに接続される。 1 個のオブジェクトとして容易な管理のために一意の構成入力がサポートされなければならない。 従って、1 個のユニットがスタック･マスターとして動作するように選ばれる。 次の節ではスタック･マスター選定プロセスのためのポイントを加える。

スタック･マスター選定のポイントは次のようにまとめられる::

1. 他のスイッチが同じスタックになければ現在スタックマスターであるスイッチ。
2. 管理者が最高のユーザープライオリティを特定してスタックマスターになるスイッチを選ぶことができる。
3. 最長のアップタイムのスイッチが選ばれる。
4. 最小の MAC アドレスのあるスイッチが選ばれる。

i

- 再選定プロセスは次のうちいずれかのイベントが生じる場合実施される:

a) スイッチ･スタックがリセットされる。

b) スイッチマスターがスタックシステムにもはや存在しない。(スタックから削除されたか電源を切るのに失敗した)

c) システムかスイッチスタックにある追加の電源の入ったスタンドアローンスイッチによってスイッチスタックのメンバー登録が増えた。

- ユーザーがスイッチのプライオリティを変えたとき、スイッチが再起動ないし再選定後に、新プライオリティがマスターの選定手順に適用されます。

- スイッチのプライオリティが無効になった場合、そのスイッチはスタックマスターとしては選定されません。

- スタックの非マスターメンバーとして設定されたスイッチはそのスタックシステムにスタックマスターがないのでない限り、起動の際マスターになろうと競合しません。

- 1 個以上のスタックマスターがスタックにあれば、プライオリティの高いもの(あるいは最長のアップタイム、最小のMACアドレスを持つもの)がスタックマスターになります。(これは通常のケースではありません。あるユニットをスタックに追加する通常の手続きは先ずスタッキングケーブルを接続し、電源を入れて 20 秒後に起動する) 2 つのスタックマスターがスタックにあれば、スタックで 1 個のみスタックマスターを選ぶために再選定の手順が実行されます。再選定手順のあと、新しいスタックマスターは以前のものとは異なります。その結果、スタックの全メンバーは新しいスタックマスターにより再構成されます。(それは元々の構成は失われることを意味します。) その間は、スタックのトラフィックは中断されます。

- 現在のスタックマスターより高いプライオリティか低いMACアドレスのスイッチをスタックへ接続し起動すると、このスイッチは常にスタックメンバーとなります。スタックマスターとするスイッチに対し最高のプライオリティの値を割当ててください。これで再選定が起きたらそのスイッチがスタックマスターとして必ず再選定されます。

- スタックマスターのものとは異なるファームウェアがあるスイッチはスタックシステムに参加できません。

6.4 ファームウェアのアップグレードと配布プロセス

PG-SW111 はファームウェアのアップグレードに 2 つの方法を提供し、1 つはXMODEM により、他方はTFTP/FTPによる。ファームウェアのアップグレードはスタック･マスターでのみ実行できる。

アップグレードプロセス

ファームウェアのアップグレードがスタック･マスターで完了すると、スタック･マスターはすべてのスタック･メンバーに向けてダウンロードされたコードを自動配布してスタック内のすべてのメンバーが同じファームウェア･バージョンで実行する。アップグレードされたコードを実行するためにはスタック･マスターを含むスタック内のすべてのメンバーを再起動することが必要ないし推奨される。

配布プロセス

ファームウェアの配布もスタック･マスターからのみ手動で許可される。スタック･マスターは現在実行中のコードをスタックリンクを通してスタック全体のメンバーまたはスタックの特定メンバーに配布できる。スタックマスターはこの機能をスタックのメンバーのファームウェアのバージョンと同期させるのに使うことができます。たとえば、異なるファームウェアバージョンのスイッチはそのスタックに接続されます。実際には、このスイッチはファームウェアのバージョンの不一致のためにスタックには加えられません。このスイッチをスタックに参加させる唯一の方法はスタックマスターからファームウェアの配布を実行することです。ファームウェアがスイッチへ分配されたのち、ユーザーが更新したファームウェアを読み込ませるには、アップグレードしたスイッチが必要です。

自動アップグレード･プロセス

ファームウェアの自動アップグレード機能はユーザーが自動アップグレード機能を有効化すればスタック･メンバーのためにサポートされています。異なるファームウェアバージョンのスイッチがスタックに追加されたとき、スタックマスターは現在実行しているファームウェアをフラッシュROMからこのスイッチへダウンロードします。自動アップグレードの手順は始まるまでに数秒～数分待ちます。自動アップグレード手順が完了したら、スイッチは完全な機能を再読込みスタックに再参加するように求められます。自動アップグレード機能にはひとつ例外があります。バージョンの高いファームウェアを持つ新しいスイッチがスタックに追加されると、自動アップグレードが有効化されていてもスタックマスターは自動でファームウェアのアップグレードをすることはしません。そのかわり、スタックマスターはユーザーに最低限必要なファームウェアのバージョンをメッセージで指示します。その後ユーザーはスタックマスターとスタックメンバー全体のための新しいファームウェアを提供されたCLIコマンド群を用いてこの新しいファームウェアバージョンにより手動でアップグレードすることを選べます。

スタッキングシステムは、スタッキングシステム全体は新しく追加されるスイッチにより変更されたり影響を受けたりしないよう設計されています。

6.5　電源供給のポイント

同時に 20 秒以内に電源オンされたスタック･メンバーはスタック･マスター選定に参加し、スタック･マスターになる可能性がある。同時に 20 秒以内に電源オンされたスタック･メンバーが最初の選定に参加しない場合、再選定が行われ、すべてのスタック･メンバーは再選定プロセスに必ず参加させられる。

この新しいスタックマスターは数秒後に利用できるようになります。その間は。スイッチスタックはネットワークの混乱を最小化するため転送テーブルを使います。

スタックのスイッチに電源を投入する前に以下のガイドラインを考慮してください。ガイドラインの目的は新しいスイッチをスタックシステムへ追加したとき、スタックマスターが変更されるのを防ぐことです。スタックマスターが変更された場合、トラフィックは中断され構成が失われることがあります。(マスター選定手順のセクションを参照)　最初のインストールについては、このスイッチがスタックシステムのスタックマスターになる場合、スイッチに最高のプライオリティを設定することをお奨めします。

1. はじめてスイッチに電源を投入する順序はスタックのマスターになるスイッチに影響します。
2. 特定スイッチをスタックマスターにする場合、そのスイッチの電源から先に投入します。このスイッチがスタックマスターとなりマスター再選定が要求されるまでスタックマスターのままです。約 20 秒後、他のスイッチの電源を入れます。
3. 既存スタックへ追加するスイッチは電源投入後 20 秒以内にスタッキングケーブル経由でスタックに接続されることが必要です。
4. 電源の入ったスイッチを追加すると、追加するスイッチスタックのスタックメンバーの間で新しいスタックマスターを再選定させます。残りすべてのスイッチは新しいスタックマスターにより再構成されます。スタックマスターが当初と異なる場合、トラフィックは再構成中は中断されます。
5. スタックマスターを削除すると新しいスタックマスターが再選定されます。残りすべてのスイッチは新しいスタックマスターにより再構成されます。トラフィックは再構成中は中断されます。
6. 非リングトポロジーからスタックメンバーを削除すると、スイッチスタックは 2 個以上のスイッチスタックへ分割されます。各スタックは同じ構成です。このためネットワークで IP アドレスの構成対立が生じます。スイッチスタックを個別に分離させておく場合、IP アドレスか新たに作成したスイッチスタックのアドレスを変更します。スイッチスタックを分割させない場合は：

   a) 新しく作成したスイッチスタックの電源を切る

   b) スタッキングポートを通じて当初のスイッチスタックへ再接続させる。

   c) 電源を再投入する。

ケース　1: 同じファブリックの内部スタッキング･リンクにより 2 つのスイッチをスタックする

たとえば、CB1 とCB2 をスタックするとする。 CB1 をスタック･マスターとする場合、最初にCB1 をプラグインする必要がある。その 20 秒後にCB2 をプラグインする。

Fabric 1	SWM1 ◄─►	SWM2
Fabric 2		
Fabric 3		
Fabric 4		

ケース　 2: 異なるファブリックの外部スタッキングリンクにより 2 つのスイッチをスタックする

たとえば、CB1 とCB3 をスタックするとする。 CB1 をスタック･マスターとする場合、最初にCB1 をプラグインする必要がある。その 20 秒後にCB3 をプラグインして、20 秒以内にCB1 とCB3 を外部スタック･ケーブルで接続する。

Fabric 1	▲ SWM1	
Fabric 2	▼ SWM3	
Fabric 3		
Fabric 4		

ケース　 3: 内部と外部スタッキングリンクを使い 4 つのスイッチをスタックする

たとえば、CB1, CB2, CB3,とCB2 をスタックするとする。

まずスタック･マスター (CB1)にするSWMをプラグインしてから、20 秒後にCB2 をプラグイン(ケース 1 参照)する必要がある。 次に、CB3 をプラグインして、20 秒以内にCB1 とCB3 を外部スタック･ケーブルで接続する。 CB4 をプラグインして、最後にCB2 とCB4 を外部スタック･ケーブルで接続する。

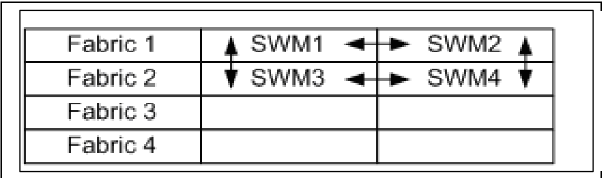
Fabric 1	▲ SWM1 ◄─►	SWM2 ▲
Fabric 2	▼ SWM3 ◄─►	SWM4 ▼
Fabric 3		
Fabric 4		



初回のインストール時には、以上の電源供給配慮に従うこと。さもないとどのCBがマスターになるか決まらない (マスター選定プロセスの項目を参照) 。構成を保存した場合には、同時に電源をオンしてもかまわない。しかし、外部スタック･ケーブルは電源投入中は常時存在しなければならない。

ケース　4:スタックから故障したスタック·メンバーを交換する

たとえば、CB1、CB2、CB3、及びCB4 がスタック·システムを構成し、CB1 がスタック·マスター、残りがスタック·メンバー、CB4 が故障しているとする。スタック·システムに影響無くCB4 を直接取外せる。次に、CB4 があった場所に新たなCBをプラグインしてCB2 とCB4 を外部スタック·ケーブルで接続する。 CB4 の再起動後、これはスタック··メンバーとなる。

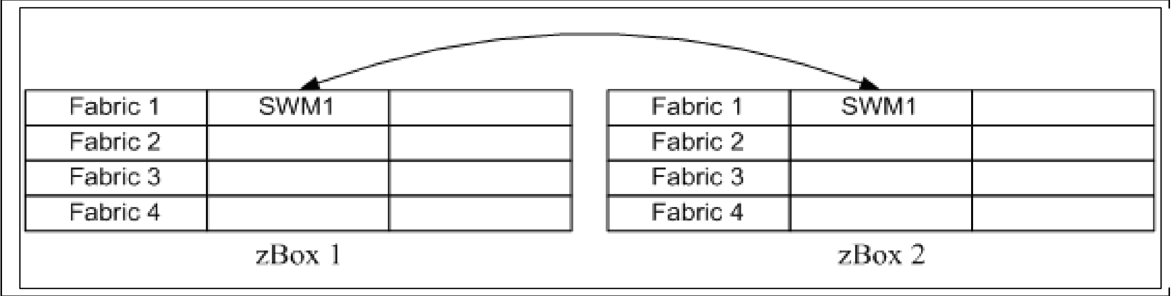


ケース　5: 故障したスタック·マスターをスタックから交換する(故障したものがスタック·マスターであれば、残りのスタック·メンバーは新たなスタック·マスターをその中から選定することを意味する)

スタック·マスターであるCB1 が故障し、CB1 が動作しなくなった後CB2 がスタック·マスターになると仮定する。CB1 から外部スタック·ケーブルを外し、ファブリックからCB1 を取外す、次にCB1 があった場所に新たなCBをプラグインしてから、CB1 とCB3 を外部スタック·ケーブルで接続する。 CB1 の再起動後、これがスタック·メンバーとなる。CB1 をスタック·マスターにする必要があれば、CB2(スタック·マスター)から"switch movemangement <fromunit><tounit>"コマンドでスタック· マスターをCB2 からCB1 に移動する。

ケース　6: 2 つのシャーシを横断して 2 つのスイッチをスタックする

zBox 1 にある CB1 がスタック·マスターであるとすると、zBox 1 にCB1 を最初にプラグインする 必要がある。 次にzBox 2 にCB1 をプラグインしてから、20 秒以内にスタック·ケーブルを接続する。



6.6 スタック・メンバーのプロビジョニング

この機能によりスイッチがスタックに参加する前にオフラインで構成できます。スイッチIDは未使用の数字 1 から 8 の最小の数字を自動的に割当てられます。通常はmove managementコマンドでスタックを構成するか、再 選定しない限り、スタックマスターは最低IDのスイッチを取ります。

独自のメンバー番号(スイッチID)でスタックマスターからスタックメンバーを作成でき、現在スタックの一部でないこの事前に構成されたスイッチに機能を予め構成します。同一モデルのスイッチをスタックに追加する場合、新しいスイッチは同じメンバー番号(スイッチID)を使おうとしているので、新しいスイッチはスタックマスターにより事前に構成/セットアップされた構成を適用されます。

6.7 名前付けの仕組み

スタックメンバーのネーミングスキームがこのセクションで解説されます。これにより特定のスイッチモジュール及びスイッチモジュールの一部を容易に識別して操作できます。

MMBはISMICにより以下の情報をスイッチが読み取れるように提供しなければなりません;

1. **ラック名 (読み出しのみ): 今後のために予約されており、空である。**
2. **ボックス名** (読み出しのみ): MMB は“Rack1-Encl1-CB1/1/1”の FRU データから連番を取得しこれを“Rack1-Encl1-CB1/1/1”名とする。 (この名前は一意でなければならない。)
3. **ベイ番号** (1-8) (読み出しのみ): MMB により ISMIC を通して静的ベイ番号が割当てられる。
4. **SWM ユーザー定義名** (Read・Write): この欄はこの名前がウェブ UI からスイッチへアクセスするためスイッチのホスト名としてのみ使われ、DNS 名として使われることもあります。

6.7.1 スイッチ名

スイッチの名前はイーサネット・コネクション・ブレードのユーザーに割当てられた名前をその名前に使います。このデフォルト名はMMBまたはスイッチにより利用できるインターフェイス(CLI/Web UI)を通して変更でき 、ISMICメモリへ書き込まれます。イーサネット・コネクション・ブレードの起動段階では、この名前をホスト名として読み込み、DNS名として使われます。(注記:DNS名はDNSクライアントがサポートされているときにのみ有効です。

MMBにより特定される名前が無い場合、構成ファイルにある名前をホスト名として使います。

6.7.2 スタック内の名前付けとアドレス割当て

イーサネット・コネクション・ブレードがシャーシにプラグインされるにともないMMBは必要な名前付け情報を準備しなければならない。 イーサネット・コネクション・ブレードがManagement Blade (MMB)から電源を投入されると、この情報をISMICを通して読み込む。

MMBはイーサネット・コネクション・ブレードの識別子として<ラック名>-<“Rack1-Encl1-CB1/1/1”名>-CB<ベイ番号>(または<ラック名>が識別されない場合<“Rack1-Encl1-CB1/1/1”名>-CB<ベイ番号>)を使用し、イーサネット・コネクション・ブレードへのISMICのSWMユーザー定義名欄にこの識別子を指定する。 イーサネット・コネクション・ブレードはこの名前"<ラック名>-<“Rack1-Encl1-CB1/1/1”名>-CB<ベイ番号>/<スロット番号>/<ポート>"を使用してイーサネット・コネクショ ン・ブレードのポートを操作する。<スロット番号>/<ポート>の部分は物理ポートまたは論理ポート (ポートチャネル) の識別に使用される。たとえば、ボックス 1 とベイ 1 の最初のポートチャネルは“Rack1-Encl1-CB1/1/1”として表記される。

7　E-KEY機能の特長

この節はイーサネット・コネクション・ブレードの全体的メカニズムと要件を含みE-KEY機能の情報を説明する。

MMBはブレード・シャーシ全体の構成を監視できる中央管理部である。 従ってMMBは、イーサネット・コネクション・ブレード、メザニン、及びCPUブレードのE-KEY有効化と無効化機能を制御するE-KEYアプリケーションを実行している。MMBは一方ではIPMIを通してサーバ・ブレード上のBMCに作用してCPUブレードとメザニン・カードのポートを無効化/有効化する。 MMBは他方ではISMICを通してイーサネット・コネクション・ブレードに情報を与え、イーサネット・コネクション・ブレードのダウンリンク・ポートを有効化/無効化する。 イーサネット・コネクション・ブレードへの互換性のあるサーバ・ブレードとメザニンの接続のみコネクション・ブレードの電源オンの際MMBのE-KEYプロセスにより有効化される。 この初期化手順の後、E-KEYプロセスは有効化されたポートをサーバ・ブレード/メザニンまたはコネクション・ブレードのインストール変更に従い最終的に更新する。

1. E-KEY 機能は次のようなメカニズムである：E-KEY イーサネット・コネクション・ブレードの未使用ダウンリンク・ポートを無効化する
2. 互換性のあるメザニンカードや CPU ブレードポートに接続されたイーサネット・コネクション・ブレードのダウンリンクを無効化する。
3. イーサネット・コネクション・ブレードの互換性あるダウンリンクに接続されたすべてのメザニンカードや CPU ブレードチャンネルを無効化する。
4. 互換性のある信号レベルによるハードウェアの問題と誤ったエラーメッセージを防止する。

イーサネット・コネクション・ブレードの動作：

1. KEY 機能はイーサネット・コネクション・ブレードで利用できるすべての構成された機能の可用性と操作性が保持されるように実現される。
2. E-KEY 有効化/無効化機能はイーサネット・コネクション・ブレード(のシャットダウン/非シャットダウン) メザニン・カード(有効化/ 無効化)の既存の利用可能なポート有効化/無効化機能とは無関係である E-KEY。
3. E-KEY 有効化/無効化機能は標準イーサネット・コネクション・ブレード/メザニン・カードのポート有効化/無効化機能とは無関係でこれらより「低い」”低レベル物理層機能”として実現される E-KEY。
4. イーサネット・コネクション・ブレードのユーザーインターフェイスすべて (CLI/WebUI)を拡張してダウンリンク・ポート E-KEY 状態を表示できる。

イーサネット・コネクション・ブレードのポートがE-KEY機能により無効化されると、ユーザーによりイーサネット・コネクション・ブレードポートでは有効化できない。しかしユーザーはこれらのポートに通常のスイッチング機能を構成できる。これらのポートがE-KEY機能により再び有効化されるとユーザーはこれらのポートを有効化も無効化もできる。

ポートがE-KEY機能により無効化されてもユーザーはこのポートに何らかの機能を構成できる。 しかしこのポートはリンクステート機能等ある機能のために内部でファームウェアにより無効化されていることがある。 この場合、当該ポートはE-KEY機能により再び有効化されても無効なままとなる。

8　ウェブ･ベース管理インターフェイス

8.1　概　要

BX900 ネットワーク･スイッチ･ブレードはマイクロソフト･インターネットエクスプローラーやファイアフォックス等の標準のウェブブラウザにより、遠隔で構成や管理ができる内蔵のソフトウェアインターフェイスを提供します。 このソフトウェアのインターフェイスはネットワークスイッチのシステムの監視と管理も可能にします。このネットワークスイッチをコンソールから初めて構成するときには、IPアドレスとサブネットマスクをネットワークスイッチへ割当てなければなりません。その後で、スイッチのIPアドレスをアドレスバーへ入力して、ネットワークスイッチのウェブソフトウェアインターフェイスへ直接アクセスできます。このように、ネットワークスイッチのコンソールポートにあたかも直接接続されているように、リモートPCステーションからウェブブラウザでスイッチを管理できます。

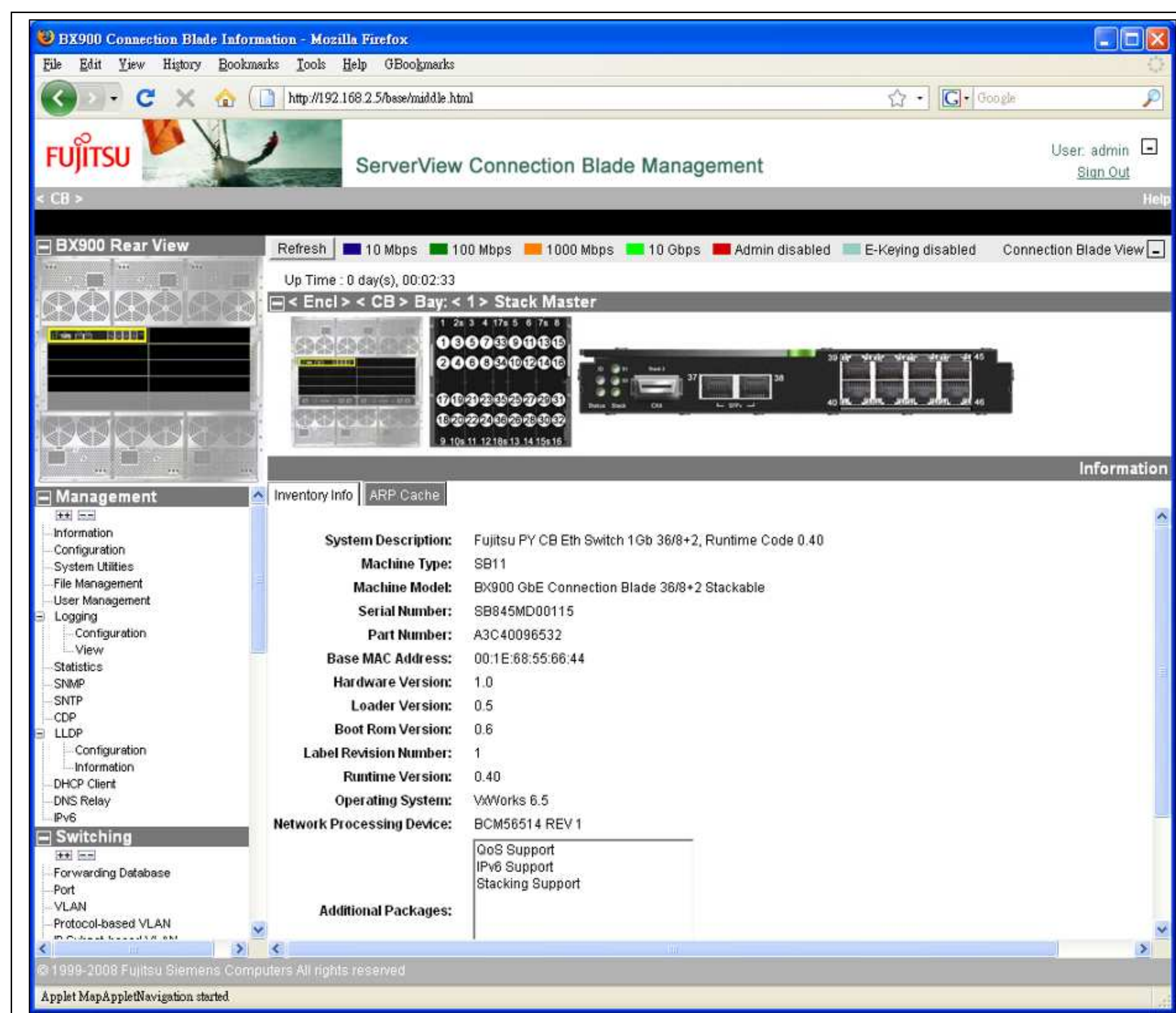


図 ： ウェブ管理インターフェイス

8.1.1 メニュー･オプション

利用できるメニューオプションは;管理、グループ管理、セキュリティ、QoS、スタッキングです。

1. **管理メニュー:**

   この節はSNMPとトラップマネージャ、ピング、DHCPクライアント、SNTP、システム時間を構成する、Telnet セッ ションとコンソールのボーレートを含めたパラメータを定義する、スイッチモジュールソフトウェアをダウンロードする、スイッチモジュール、スイッチ統計、レイヤー2 のMACアドレス等をリセットする、等の情報を提供します。

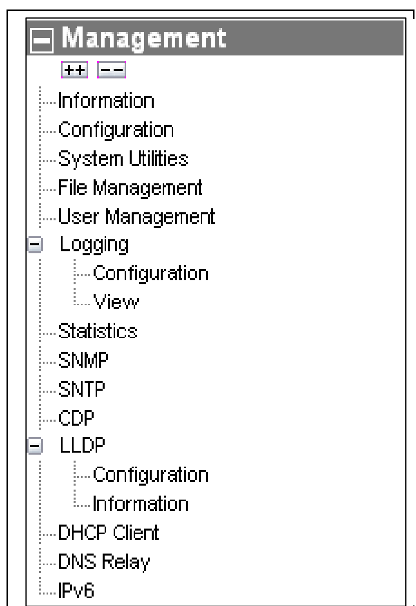


図: 管理メニュー

2. **スイッチングのメニュー:**

この節はユーザーが、スイッチポートベースのVLAN、プロトコルベースのVLAN、GARP、IGMPスヌーピング、ポートチャンネル、スパニングツリー、802.1pプライオリティマッピング、及び、ポートセキュリティ等を構成できるようにします。

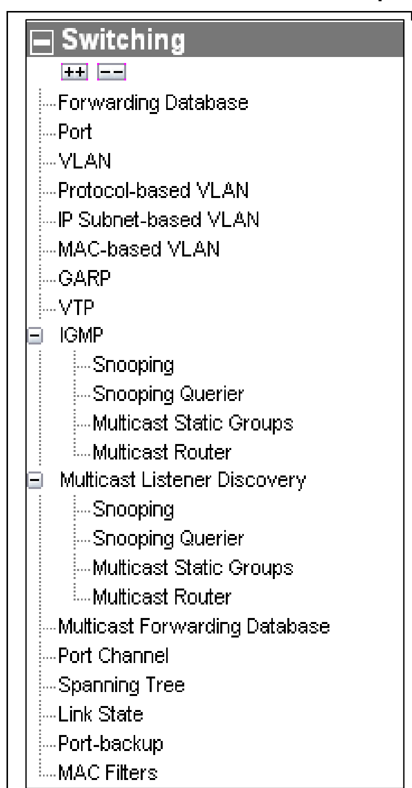


図: スイッチングのメニュー

3. **セキュリティ・メニュー:**

この節はユーザーが 802.1x、RADIUS、TACACS、LDAP,アクセス制御リスト、IPフィルター、セキュアHttp、セキュア・シェル等を含むスイッチのセキュリティを構成できるようにします。

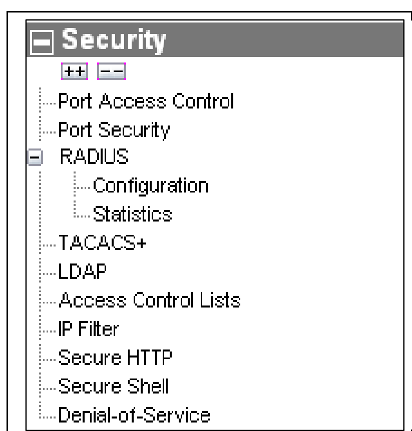


図: セキュリティ・メニュー

4. **QoS メニュー:**

この節は、DiffServとCoSの構成方法を説明する。



図: QoSメニュー:

5. **スタッキングのメニュー(スタックできるイーサネット・コネクション・ブレード)**

この節は、装置のスタックとスタック化装置の実行時コードの更新の構成方法を説明する。

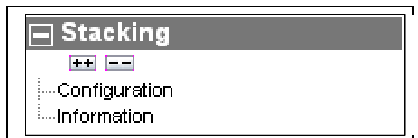


図: スタック・メニュー

8.2 管理メニュー

この節はSNMPとトラップマネージャ、ピング、DHCPクライアント、SNTP、システム時間を構成する、Telnet セッション とコンソールのボーレートを含めたパラメータを定義する、スイッチモジュールソフトウェアをダウンロードする、スイッチモジュール、スイッチ統計、レイヤー2 のMACアドレス等をリセットする、等の情報を提供します。

8.2.1 情報

8.2.1.1 インベントリ情報

Information

Inventory Info

System Description:	FSC PRIMERGY BX900 GbE Connection Blade 36/12, IBP, Runtime Code 0.30
Machine Type:	SB11A
Machine Model:	BX900 GbE Connection Blade 36/12
Serial Number:	SQ903LW00182
Part Number:	A3C40096531
Base MAC Address:	00:23:8B:57:50:9E
Hardware Version:	1.0
Loader Version:	0.6
Boot Rom Version:	0.8
Label Revision Number:	1
Runtime Version:	0.30
Operating System:	VxWorks 6.5
Network Processing Device:	BCM56312 REV 1
Additional Packages:	QoS Support IPv6 Support

Module	Type	Status	Ethernet Compliance Codes	Vendor				
				Name	Part No.	Serial No.	Revision No.	Manufacturing Date

Re

図:インベントリ情報

このパネルにより工場で非揮発性メモリに記憶されたスイッチの非常に重要な製品データを表示します。

構成不可能なデータ

- **System Description -** このスイッチの製品名
- **Machine Type-** このスイッチのマシンタイプ
- **Machine Model -** マシンタイプ内のモデル
- **Serial Number -** このスイッチのシリアル番号
- **Part Number -**製造パーツ番号

Base MAC Address - MACアドレス

Hardware Version - このスイッチのハードウェアのバージョン。1番目のバイトがメジャーバージョンを2番目がマイナーバージョンを表します。

Loader Version - 現在スイッチで実行されているローダーコードのリリースバージョンメンテナンス番号。たとえばリリースが1でバージョンが2なら、形式は「1.2」です。

Boot Rom Version - 現在スイッチで実行されているブートROMのリリースバージョンメンテナンス番号。たとえばリリースが1でバージョンが2なら、形式は「1.2」です。

Label Revision Number - ラベルのリビジョンシリアル番号。

Runtime Version - 現在スイッチで実行されているコードのリリースバージョンメンテナンス番号。たとえばリリースが1でバージョンが2なら、形式は「1.2」です。

Operating System - 現在スイッチで実行され ている オペレー ティング システム

Network Processing Device - ネットワークプロセッサのハードウェアを識別します

Additional Packages - あるならば、スイッチにインストールされたオプションのソフトウェアパッケージ。たとえば、QoS、IPv6、あるいはスタッキングサポート

Module - SFPモジュール名

Type - SFPの種類

Status - SFPのステータス

Ethernet Compliance Codes - トランシーバのコード

Vendor Name - SFPトランシーバーのベンダー名は、企業の正式名、一般 に受け入れられ ている企業名の略称、企業のSCSI会社コード、あるいは企業の証券取引コードでなければなりません。

Vendor Part Number - SFPトランシーバーのベンダーが提供するパーツ番号

Vendor Serial Number - ベンダーが指定するシリアル番号

Vendor Revision Number - ベンダーが提供するパーツ番号の改訂レベル

Vendor Manufacturing Date - 製造年月日

コマンドボタン

Refresh - 頁を最新情報で更新する

8.2.1.2 ARP キャッシュ

アドレス解決プロトコル(ARP)は物理(MAC)アドレス(データリンクレイヤー)をIP(ネットワークレイヤー)アドレスへ動的にマッピングします。このパネルはARPキャッシュの現在の内容を表示します。

各コネクションについて次の情報が表示されます;

- 物理(MAC)アドレス
- 関連付けられたIPアドレス
- 接続に使われるポートの識別

Information

Inventory Info | ARP Cache

MAC Address	IP Address	Slot/Port
00:07:E9:07:73:EA	192.168.2.188	Management

Refresh Clear All

図:ARPキャッシュ

コマンドボタン:

Refresh - 最新のデータでページを更新する

Cear All - システムARPテーブルのすべてのMAC入力を削除する

8.2.2 構成

8.2.2.1 システム内容

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

System Description: FSC PRIMERGY BX900 GbE Connection Blade 36/12, L2+ Switch, Runtime Code 0.14
System Name:
System Location:
System Contact:
In-Band Mgmt IP Address: 0.0.0.0
Out-of-Band Mgmt IP Address: 192.168.2.5
System Object ID: 1.3.6.1.4.1.231
System Up Time: 0 days, 0 hours, 1 mins
Current SNTP Synchronized Time: Not Synchronized

Apply

図: System Description

構成可能データ

System Name - このスイッチを識別するために使う名前を入力します。31 字までの英数 字が使えます。 工場側デフォルト値は空白である。

System Location - このスイッチの場所を入力します。31 字までの英数字が使えます。工場側デフォルト値は空白である。

System Contact - このスイッチの担当者の連絡先 31 字までの英数字が使えます。工場側デフォルト値は空白である。

構成不可能なデータ

System Description - このスイッチの製品名

In-Band Mgmt IP Address - インバンド管理(外部ポート経由でアクセスされる)に割当てられたIPアドレス

Out-of-Band Mgmt IP Address - out-of-band管理(MMBサービスポート経由でアクセスされる)に割当てられたIPアドレス

System Object ID - システムのエンタープライズMIB用のベースオブジェクトID

System Up time - 最終のスイッチの再起動以来の経過日数、時間、分

Current SNTP Synchronized Time - UTCで現在同期化ずみのSNTP時間を表示する。時間が同期化されていない場合、「同期化されていません」と表示します

コマンドボタン

Apply - 画面の値で更新する。 パワー・サイクル後も保持させるには保存を実行する画面の値で更新する。 パワー・サイクル後も保持させるには保存を実行する。。

8.2.2.2　**インバンド管理**

インバンド管理は任意のスイッチのフロントパネルポート経由でスイッチにインバンド接続することに使われる論理的なインターフェイスです。スイッチのインバンド管理と関連する構成パラメータはトラフィックがスイッチまたはルーティングされるフロント･パネル･ポートの構成に影響しません。

ネットワークでスイッチにアクセスするにはまずIP情報 (IPアドレス、サブネットマスク、及び、 デフォルトゲ ートウェイ)を構成しなければなりません。以下の項目からいずれかを使用してIP情報を構成できます:

- BOOTP
- DHCP
- EIA-232 ポートを介すする端末インターフェイス (MMBからコンソール･リダイレクトによる)

インバンド接続を確立したら、次のどの手段でもIP情報を変更できる:

- EIA-232 ポートを介する端末インターフェイス
- Telnetによる端末インターフェイス
- SNMPによる管理
- ウェブによる管理

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

IP Address:* 0 . 0 . 0 . 0
Subnet Mask:* 0 . 0 . 0 . 0
Default Gateway:* 0 . 0 . 0 . 0
IPv6 Address:
Burned In MAC Address: 00:23:8B:17:7B:85
In-Band Mgmt Protocol: None
DHCP6 Client: Disable
Management VLAN ID:* 1
Web Mode: Enable
Java Mode: Enable
Web Port:* 80

* = mandatory

Apply

図:　In-Band Mgmt Config

選択基準

In-Band Mgmt Protocol - 　電源投入後スイッチが何をすべきかを指定します :Bootp要求を送信する、DHCP要求を送信する、またはなにない(なし)。工場出荷時デフォルトは「なし」です。インバンドとout-of-band管理の両方に対してこれを選択できません。 OOBインターフェイスで構成された プロトコルがBootpまたはDHCPに構成されている場合ここでは「なし」を選ぶことしかできません。

DHCP6 Client - DHCP6 の有効化または無効化を選びます。インバンド管理とout-of-band管理の両方は選べません。out-of-band管理が無効化されている場合ここでは有効化のみ選べます。

Web Mode - 　スイッチがウェブブラウザからアクセスできるかどうかを指定します。ウェブモードを有効化すればウェブブラウザからスイッチを管理できます。工場出荷時のデフォルトは有効化されています。

Java Mode -画面の右上にスイッチの画像を表示するJAVAアプレットを 有効化または無 効化する。アプレットを

実行している場合画面左側のナビゲーションツリーを使わずにスイッチの画像をクリックして構成画面を選択できるようになります。

構成可能データ

IP Address - インターフェイスのIPアドレス 工場側デフォルト設定値は 0.0.0.0 である。

Subnet Mask - インターフェイスのIPサブネットマスク 工場側デフォルト設定値は 0.0.0.0 である。

Default Gateway - IPインターフェイスのデフォルト・ゲートウェイ工場側デフォルト設定値は 0.0.0.0 である。

インバンド管理とOOB管理ともにデフォルト・ゲートウェイを設定することはできない。 OOB管理用ゲートウェイが 0.0.0.0 に構成されていればゲートウェイを変更できる。

Management VLAN ID - スイッチの管理VLAN IDを指定します。1 から 4094 までの任意の数値を指定できます。管理VLANはスイッチの管理に使われます。この欄は管理権限のあるユーザーが構成でき、他のユーザーは読み取り専用です。

Web Port - この選択欄はHTTPポート番号を設定するために使用する。 その値は 1～65535 の範囲でなければならない。Port80 がデフォルト値である。 ウェブページが表示されると現在の構成値が表示される。

構成不可能なデータ

Burned-in MAC Address - MACアドレスはローカルで管理されるアドレスを構成しないことを選択した場合にインバンド接続に使用される。

IPv6 Address - IPv6 アドレスを表示する

コマンドボタン

Apply - 画面の設定をスイッチに更新します。電力サイクルで新しい値をスイッチに保持させるには保存してください。

8.2.2.3 Out-of-Band管理

Out-of-Band管理インターフェイスはMMBサービス･ポートを通してネットワーク･ アクセス接続を提供する。

Configuration
System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

IP Address:* 192 . 168 . 2 . 5
Subnet Mask:* 255 . 255 . 255 . 0
Default Gateway:* 0 . 0 . 0 . 0
IPv6 Address: FE80::223:8BFF:FE17:7B86/64
OOB Interface Configured Protocol: None
DHCP6 Client: Disable
Burned In MAC Address: 00:23:8B:17:7B:86
* = mandatory
Apply

図:アウトオブバンド管理Configを

このパネルによりout-of-band管理を使うネットワーク上でのスイッチと通信するために必要なパラメータを指定します。

選択基準

OOB Interface Configured Protocol - 電源投入後スイッチが何をすべきかを指定します:Bootp要求を送信する、DHCP要求を送信する、またはなにない(なし)。工場出荷時デフォルトは｢なし｣です。インバンドとout-of-band管理の両方同時に選択できません。 インバンド管理がBootpまたはDHCPに構成されている場合ここでは｢なし｣のみとなります。

DHCP6 Client - DHCP6 の有効化または無効化を選びます。インバンド管理とアウ トバンド管 理の両方に選 ぶことはできません。インバンド管理が無効化されている場合ここでは有効化のみとなります。

構成可能データ

IP Address - インターフェイスのIPアドレス , 工場側デフォルト設定値は 0.0.0.0 である。

Subnet Mask - インターフェイスのIPサブネットマスク工場側デフォルト設定値は 0.0.0.0 である。

Default Gateway - IPインターフェイスのデフォルト･ゲートウェイ 工場側デフォルト設定値は 0.0.0.0 である。デフォルトゲートウェイはインバンド管理とOOB管理ともに設定できない。インバンド管理用ゲートウェイが 0.0.0.0 に構成されていればゲートウェイを変更できる。

構成不可能なデータ

Burned In MAC Address - 焼付けMACアドレスはOOB接続に使用される。

IPv6 Address - IPv6 アドレスを表示する

コマンドボタン

Apply - 画面の設定をスイッチに更新します。パワーサイクル後、設定を保持するにはスイッチに保持してください。

8.2.2.4 Telnetセッション

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

Telnet Session Timeout (minutes) (1 to 160):* 5
Maximum Number of Telnet Sessions: 5
Allow New Telnet Sessions: Yes
Telnet Server Admin Mode: Enable
Password Threshold (0 to 120):* 3

* = mandatory

Apply

図 : Telnetセッション・コンフィグ

選択基準

Maximum Number of Telnet Sessions - 同時に許可するTelnetセッション数をプルダウン・メニューから選択する最大セッション数は 5 であり、これはデフォルト値でもある。

Allow New Telnet Sessions - これをNoに設定すると、新たなTelnetセッションは許可されなくなる。 デフォルト設定は可能 (Yes) である。

Telnet Server Admin Mode - インバンドTelnetセッションの管理モード この値を無効化に設定するとTelnetポートを遮断する。管理モードが無効化されていると、すべての既存のTelnet接続が切断される。 デフォルト値は有効である。

構成可能データ

Telnet Session Timeout - Telnetセッションで動作が無い場合セッションがログオフされるまでの分数を指定する。1～160 の範囲で任意の数字を入力できる。デフォルト値は 5 である。

Password Threshold - ログオン試行の回数限度にコンソール・ポートで到達すると、システム・インターフェイスは次のログオン試行を許可するまでは所定時間応答を止める。 (silent time コマンドでこの間隔を設定する。) Telnetでこの閾値に到達するとTelnetのログオン・インターフェイスは閉じる。

コマンドボタン

Apply - 画面の設定をスイッチに更新します。パワーサイクル後、設定を保持するには保存してください。

8.2.2.5 Telnetクライアント･コンフィグ

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

Admin Mode: Enable
Maximum Sessions: 5
Session Timeout(minutes) (1 to 160):* 5
Terminal Length (10 to 100):* 24
* = mandatory

Apply

図: Telnetクライアントの構成

選択基準

Admin Mode - アウトバウンドTelnetサービスが有効化または無効化されているかを指定する。 デフォルト値は有効化である。

Maximum Sessions - 許容最大アウトバウンドTelnetセッション数を指定する。 デフォルト値は 5 である。値の有効範囲は 0 から 5 である。

構成可能データ

Session Timeout - アウトバウンドTelnetのログイン試行無しのタイムアウトを指定する。 デフォルト値は 5 である。値の有効範囲は 1 から 160 である。

Terminal Length -コンソールの最大スクロール･ライン数を指定する。

コマンドボタン

Apply - 更新した設定をスイッチに適応します。構成の変更は即時に有効化されます。

8.2.2.6 シリアルポート

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

Serial Port Login Timeout (minutes) (0 to 160):*	5
Baud Rate (bps):	115200
Character Size (bits):	8
Flow Control:	Disabled
Stop Bits:	1
Parity:	None
Password Threshold (0 to 120):*	3
Silent Time (Sec) (0 to 65535):*	0
Terminal Length (10 to 100):*	24

* = mandatory

Apply

図：シリアルポート・コンフィグ

選択基準

Baud Rate (bps) - プルダウンメニューからシリアルポート接続のデフォルト速度を選択する。 1200、2400、4800、 9600、19200、38400、57600、115200 ボーから選択できる。 工場側デフォルト設定は 9600 である。



ボーレートを変更すると、MMBを通すコンソール・リダイレクトは機能しなくなる。

構成可能データ

Serial Port Login Timeout - スイッチが接続を切る 前に、シリアルポート接続で何分間作動中止させるかを指定します。0 から 160 の数値を入力します。工場出荷時のデフォルトは 5 です。0 を入力すればタイムアウトを無効化します。

Password Threshold - ログオン試行の回数限度にコンソール・ポートで到達すると 、システム・インターフェイスは次のログオン試行を許可するまでは所定時間応答を止める。 (silent time コマンドでこの間隔を設定する。) Telnetでこの閾値に到達するとTelnetのログ オン・インタ ーフェイスは閉じる。

Silent Time - パスワード閾値コマンドにより設定された閾値を失 敗したログオン試 行回数が超過した後、管理コンソールにアクセス不能になるまでの時間をこのコマンドで設定する。

Terminal Length - コンソールの最大スクロール・ライン数を指定する。

構成不可能なデータ

Character Size (bits) - 一文字のビット数。 この値は常に 8 である。

Flow Control - ハードウェア・フロー制御が有効化されるか無効化されるかを指定する。 これは常時無効化されている。

Stop Bits - 一文字毎のストップビット数 これは常時 1 である。

Parity - シリアルポートで使用されるパリティーの方法 これは常時無しである。

コマンドボタン

Apply - 画面の設定をスイッチに更新します。パワーサイクル後、設定を保持するには保存してください。

8.2.2.7 HTTP コンフィグ

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

HTTP Session Soft Timeout (Minutes) (0 to 60) :* 15

HTTP Session Hard Timeout (Hours) (0 to 168) :* 24

Maximum Number of HTTP Sessions (0 to 16) :* 16

* = mandatory

Apply

図： HTTP コンフィグ

構成可能データ

HTTP Session Soft Timeout - この欄はHTTPセッション の無動作タイムアウトを設定するために使用される。 その値は 0～60 分の範囲で定める。0 に設定するとタイムアウトは無限大となる。デフォルト値は 15 分である。ウェブページが表示されると現在の構成値が表示される。.

HTTP Session Hard Timeout - この欄はHTTPセッシ ョンのハード･タイムアウトを設定するために使用される。このタイムアウトはセッションの動作レベルには影響されない。 その値は 0～168 時間の範囲で定める。0 に設定するとタイムア ウトは 無 限 大となる。デフォルト値は 24 時間である。ウェブページが表示されると現在の構成値が表示される。.

Maximum Number of HTTP Sessions - この欄はHTTPセッションの 最大許容数を設定するために使用される。その値は0～16 回の範囲で定める。デフォルト値は16 時間である。 ウェブページが表示されると現在の構成値が表示される。.

コマンドボタン

Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの 変更は保存しなければパワーサイクル後は保持されません。

8.2.2.8 **DDNSコンフィグ**

図：DDNSコンフィグ

選択基準

DDNS Host - データが表示されるまたは構成される DDNSホストを選択する。 項目を追加するが選択されると、新たなDDNSホストを構成できる。

Server Type - DDNSサーバのサーバ･タイプを選択する。 次のどれでも選べる：

- EASYDNS
- DYNDNS
- DHS
- ODS
- DYNS
- ZONEEDIT
- TZO

構成可能データ

Host Name - DDNSサーバのホスト名

User Name - DDNSサーバのユーザー名

Password - アカウント用の新規オプションまたは変更パスワードで、 タイプした文字列 は表示されず、アステリスク(*)のみ見える。パスワードは最大長 32 文字で大文字と小文字は区別される。

IP Address - The IPアドレスはユーザーが設定する"ホスト名"にマップされる。

Server IP - このオプションを選択するとIPアドレスはインバンド管理 IPアドレス に設定される。

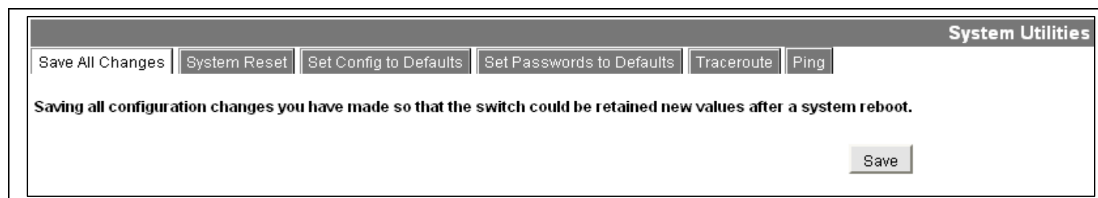
コマンドボタン

Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければ電力サイクル後、保持されません。

Remove - 選択されたDDNS構成を削除する

8.2.3 システム･ユーティリティー

8.2.3.1 すべての変更を保存する


System Utilities

Save All Changes | System Reset | Set Config to Defaults | Set Passwords to Defaults | Traceroute | Ping

Saving all configuration changes you have made so that the switch could be retained new values after a system reboot.

Save

図 ： すべての変更を保存する

コマンドボタン

Save － このボタンをクリックすれば､行った構成の変更をシステム 再起動後にも保存できます。

8.2.3.2 システムのリセット


System Utilities

Save All Changes | System Reset | Set Config to Defaults | Set Passwords to Defaults | Traceroute | Ping

Resetting the switch will cause all operations of this switch to stop. This session will be broken and you will have to log in again after the switch has rebooted. Any unsaved changes will be lost.

Reset

図 ： システムのリセット

コマンドボタン

Reset - このボタンを選んでスイッチを再起動します。最後の保存実行後、行ったすべての構成の変更は失われます｡このボタンを選んだ後には確認の画面が表示されます。

8.2.3.3　**コンフィグをデフォルトに設定する**

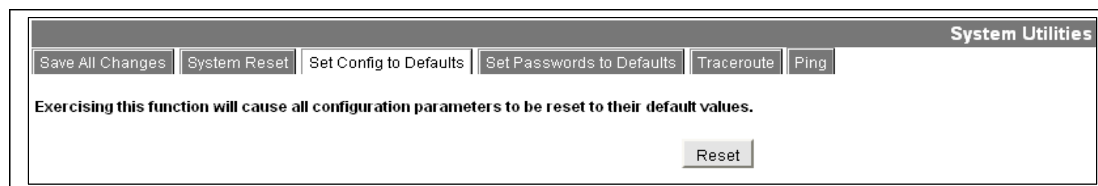


図 :コンフィグをデフォルトに設定する

コマンドボタン

Reset - すべての構成パラメータを工場側デフォルト設定値にリセットするためにはこのボタンを選択する。 これまでに行ったすべての変更は、保存を実行したとしても消去される。　このボタンを選択した後、確認画面が表示される。 .

8.2.3.4　**パスワードをデフォルトに設定する**

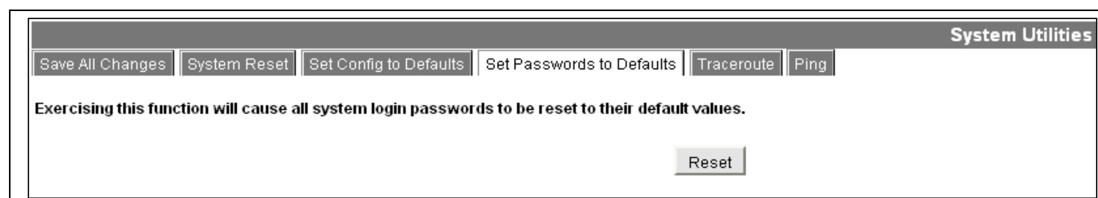


図 :パスワードをデフォルトに設定する

コマンドボタン

Reset - Resetボタンをクリックするとシステム・ログイン・パスワードをすべてデフォルト値に戻します。スイッチに新たな値を電源遮断後も保持させるには保存してください。

8.2.3.5 Traceroute

この画面によりTracerouteの要求を特定のIPアドレスへ送るようスイッチに指令します。これによりパケットが遠隔の目的地へ届くのに使うパスを発見できます。適用ボタンを押すとすぐに、スイッチはTracerouteを送り、構成可データの下に結果が表示されます

1	x.y.z.w	1 ms 2 ms 3 ms
2	0.0.0.0	0 ms 0 ms 0 ms
3	0.0.0.0	0 ms 0 ms 0 ms

System Utilities
Save All Changes | System Reset | Set Config to Defaults | Set Passwords to Defaults | Traceroute | Ping
IPv4 Address
Probes Per Hop (1 to 10):* 3
MaxTTL (1 to 255):* 20
InitTTL (1 to 255):* 1
Interval(secs) (1 to 60):* 3
TraceRoute:
* = mandatory
Apply

図: Traceroute

構成可能データ

IP Address/Host Name/IPv6 Address - スイッチにパスを発見して もらいたいステーションのアドレスを入力します。入力したアドレスは電力サイクルにより保持されません。

Probes Per Hop - ホップ毎にプローブ数を入力する 初期値はデフォルトである。 入力するホップ毎のプローブはパワー・サイクル後、保持されない。

MaxTTL - ターゲットに対する最長TTLを入力する 初期値はデフォルト値である。 入力するMaxTTLはパワー・サイクル後、保持されない。

InitTTL - 使用する初期TTL値を入力する 初期値はデフォルト値である。 入力するInitTTL はパワー・サイクル後、保持されない。

Interval - プローブ間の時間を秒で入力する 初期値はデフォルト値である。 入力する間隔秒数はパワー・サイクル後、保持されない。

コマンドボタン

Apply - traceroute.コマンドを実行する

8.2.3.6 Ping

この画面により特定のIPアドレスへピングの要求を送るようスイッチに指令します。スイッチが特定のIPアドレスと通信できるかどうかをチェックできます。適用ボタンを押すとすぐに、スイッチは 3 つのピングを送り、構成可データの下に結果が表示されます.No Reply Received from IP xxx.xxx.xxx.xxx (IP xxx.xxx.xxx.xxxから応答無し)

それ以外の場合には次が表示される：

Reply received from IP xxx.xxx.xxx.xxx (IP xxx.xxx.xxx.xxxから応答を受信した) : (send count = 3, receive count = n) (送信数=3、受信数=n)

System Utilities
Save All Changes | System Reset | Set Config to Defaults | Set Passwords to Defaults | Traceroute | Ping
Address Type: IPv4 Address
IP Address:*
Ping Output:
* = mandatory
Apply

図 ：Ping

選択基準

Address Type - IPv4 アドレス、ホスト名またはIPv6 アドレスのア ドレス･タ イプを選択する。

構成可能データ

次のオプションはユーザーが選択するアドレスに従う：

– IPv4:

IP Address - スイッチにピングしてステーションのIPアドレスを入力します。 最初の数値 は空白です。入力したIPアドレスは電源を切ると保持されません。

– ホスト名：

Host Name - スイッチにピングしてステーションのホスト名を入力します。

– IPv6:

Ping – グローバルIPv6 アドレスかリンク･ローカルアドレスをピングするために選択します。

選択するピングのタイプで次のオプションがあります:

– グローバル：

IPv6 Address - スイッチにピングしてステーションのIpv6 アドレスを入力します。

– リンク･ローカル：

Management Type - インバンド管理 または out-of-band管理を選ぶ

Link Local Address - スイッチにピングしてステーションのリンク･ローカルアドレスを入力する。初期値は空白です。

Datagram Size - データグラムのサイズを入力する 有効な範囲は 48 から 2048 までです。

Ping Output - スイッチから受信された応答結果

コマンドボタン

Apply - これでPingを初期化する

8.2.4 ファイル管理

8.2.4.1 スイッチへダウンロードする

このメニューによりファイルをスイッチへダウンロードする

File Management

Download To Switch | Upload From Switch | Start-Up File | Remove File | Copy File

File Type: Code
Protocol Mode: TFTP
FTP/TFTP Server IP Address:* 0 . 0 . 0 . 0
FTP/TFTP File Path (Source):*
FTP/TFTP File Name (Source):*
FTP/TFTP File Name (Target):*
Start File Transfer

* = mandatory

Apply

図: スイッチへファイルをダウンロードする

選択基準

File Type - ダウンロードするファイルのタイプを指定する: (ファイル·タイプのデフォルト値はコード)

- **Script** スイッチのスクリプトファイルを更新するとき構成スクリプトを特定する
- **CLI Banner** - CLIインターフェイスのバナー
- **Code** – 操作フラッシュをアップグレードするときコードを特定する
- **Configuration** - スイッチの構成を更新するとき構成を特定する。ファイルにエラーがあれ ば更新は中止されます。
- **SSH-1 RSA Key File** - SSH-1 リベスト-シャミア-エーデルマン (RSA) キーファイル **SSH-2 RSA Key PEM File/SSH-2 RSA鍵PEMファイル**- SSH-2 リベスト-シャミア-エーデルマン (RSA) キーファイル(PEMエンコード) **SSH-2 DSA Key PEM File/SSH-2 DSA鍵PEMファイル**- SSH-2 デジタル署名アルゴリズム (DSA) キーファイル(PEMエンコード) **SSL Trusted Root Certificate PEM File** - SSL 信頼されたルート証明書ファイル(PEMエンコード)
- **SSL Server Certificate PEM File** - SSL サーバ証 明書ファイル(PEMエンコード)
- **SSL DH Weak Encryption Parameter PEM File**- SSL ディフェーヘルマン脆弱暗号化パラメータ·ファイル (PEM Encoded)
- **SSL DH Strong Encryption Parameter PEM File**- SSL ディフェーヘルマン強化暗号化パラメータ·ファイル (PEM Encoded)



SSHキーファイルをダウンロードするにはSSHは管理者により無効化されなければならず、アクティブなSSHセッションがあってはならない。

Protocol Mode - ダウンロード･モードに使用するプロトコルを指定する。 FTPかTFTPから選択できる。

構成可能データ

FTP/TFTP Server IP Address - FTP/TFTPサーバのIPア ドレスを入 力する。工場出荷時デフォルトは 0.0.0.0 です。

FTP/TFTP File Path (Source) -選択したファイルがあるFTP/ TFTPサーバのパスを入力します｡96 文字まで入力できます(末尾のスラッシュも含めて)

TP/TFTP File Name (Source) - ダウンロードするファイルのFTP/ TFTPサーバの名前を入力します｡32 文字まで入力できます。

FTP/TFTP File Name (Target) -保存するファイルのスイッチ上の 名前を入力します｡30 文字まで入力できます。

Start File Transfer - ダウンロードを開始するにはこのボ ックスをチェックして 適用 ボタンを 選びます。

構成不可能なデータ

テーブルの最終行にファイル転送進捗を示す｡ 画面はファイル転送が完了するまで自動的に更新する。

コマンドボタン

Apply - 更新した画面をスイッチへ送りファイルダウンロードを実施します。

8.2.4.2 スイッチからアップロードする

このメニューを使いスイッチからコード､構成またはログファイルをアップロードします。

File Management

Download To Switch | Upload From Switch | Start-Up File | Remove File | Copy File

File Type: Code

Protocol Mode: TFTP

FTP/TFTP Server IP Address:* 0 . 0 . 0 . 0

FTP/TFTP File Path (Target):*

FTP/TFTP File Name (Target):*

FTP/TFTP File Name (Source): img61

Start File Transfer

* = mandatory

Apply

図: スイッチからファイルをアップロードする

選択基準

File Type - アップロードするファイルのタイプを特定する｡利用できるオプションは、 スクリプト､コード ､CLIバナー､構成､エラーログ､バッファーログ､トラップログです｡工場出荷時デフォルトはコードです。

Protocol Mode - アップロードするモードのプロトコルを特定する。 利用できるオプショ ンはFTPとT FTPです。

構成可能データ

FTP/TFTP Server IP Address - FTP/TFTP サーバのIP アドレスを入力する。 工場側デフォルトは 0.0.0.0 である。

FTP/TFTP File Path (Target) - アップロードするファ イルの保存先。 FTP/TFTP サーバ上のパスを指定する 最大 96 文字まで入力できる (区切りスラッシュを含む) 。 工場側デフォルト値は空白である。 .

FTP/TFTP File Name (Target) -アップロードするファ イルに付けたい名前を入力する。 最大 32 文字まで入力できる 工場側デフォルト値は空白である。 .

FTP/TFTP File Name (Source) - スイッチからアップロ ードする ファイルを特定する。

Start File Transfer - アップロードを開始するにはこの チェックボックスをオ ンしてからApplyボタンを選択する。

構成不可能なデータ

テーブルの最終行にファイル転送進捗を示す｡画面はファイル転送が完了するまで自動的に更新する。

コマンドボタン

Apply - 更新したファイルをスイッチへ送り､ファイルのアップロードを実施する。

8.2.4.3　**起動ファイル**

システムの起動に使用されるファイルを指定する。



図 ： 起動ファイル･コンフィグ

選択基準

Configuration File -構成ファイルの

Runtime File - 実行時動作コード.

構成不可能なデータ

Current Configuration File -現在の構成ファイル

Current Runtime File - 現在の実行時動作コード.

コマンドボタン

Apply - 更新した画面をスイッチへ送り､ファイルの起動を特定する。

8.2.4.4 ファイルを削除する

フラッシュメモリ内のファイルを削除する。システム起動にファイルが使用された場合、このファイルは削除できない。



図 : ファイルを削除する

選択基準

Configuration File -構成ファイルの

Runtime File - 実行時動作コード.

Script File - 構成スクリプト･ファイル

コマンドボタン

Remove - 更新した画面をスイッチへ送り､削除を実施する。

8.2.4.5　ファイルをコピーする

このメニューを使いスイッチで現在実行されている構成ファイルから起動の構成ファイルをコピーします。

File Management
Download To Switch | Upload From Switch | Start-Up File | Remove File | Copy File
File Name:*
* = mandatory
Copy to File

図　：ファイルをコピーする

構成可能データ

File Name - コピーするファイルに付けたい名前を入力する 最大 30 文字まで入力できる。 工場側デフォルト値は空白である。 .

構成不可能なデータ

テーブルの最終行にファイル･コピーの進捗を示す。画面はファイルのコピーが完了するまで自動的に更新する。

コマンド･ボタン

Copy to File -更新した画面をスイッチへ送りファイルコピーを実施する。

8.2.5 ユーザー管理

8.2.5.1 ユーザー・アカウント

デフォルトでは 2 人のユーザー・アカウントがある：

- 管理者、Read・Write特権付き
- ゲスト、Read Only特権付き

デフォルトでは管理者のパスワードは“admin”でゲストは空白である。名前は大文字と小文字の区別をしない。

Read・Write特権付きユーザー・アカウントに(すなわち、管理者として)ログオンすると、このユーザー・アカウントを用いてパスワードを割当て、デフォルト・アカウントのセキュリティ・パラメータを設定し、最大 6 個までのアカウント(管理者以外)を追加、削除できる。

User Management
User Accounts | Authentication List Config | Authentication List Summary | User Login | Login Session
User: admin
User Name:* admin
Password: •••••
Confirm Password: •••••
Access Mode: Read/Write
SNMP v3 User Configuration
SNMP v3 Access Mode: Read/Write
Authentication Protocol: None
Encryption Protocol: None
Encryption Key: Apply
* = mandatory
Apply

図: ユーザーアカウントの構成

選択基準

User - 既存アカウントを再構成する、または新たなアカウントを生成す るにはこの画面を使用できる。既存アカウントから 1 個を選択するにはこのプルダウンメニューを使用し、または'Create'を選択して新たなアカウントを追加するが、最大 5 個の'Read Only'のアカウントに到達していないことが条件である。

Authentication Protocol - 選択されたユーザー・アカウントのSNMPv3 認証プロトコ ル設定を指定する。 有効な認証プロトコルは無し、MD5 またはSHAである。無しを選択すると 、SNMPブラウザからSNMPデータにアクセスできなくなる。MD5 またはSHAを選択すると、ログイン・パスワードがSNMPv3 認証パスワードとして使用されるので、パスワードは指定しなければならない。長さは 8 文字とする。

Encryption Protocol - 選択されたユーザー・アカウントのSNMPv3 暗号化プ ロトコル設定を指定する。 有効な暗号化プロトコルは無しまたはDESである。 DESプロトコルを選択すると、Encryption Keyの欄にキーを入力しなければならない。プロトコル無しを指定した場合、暗号化鍵は無視される

構成可能データ

User Name - 新アカウントに付けたい名前を入力する (新アカウントを生成す るとき のみこの欄にデータを入力できる。)。ユーザー名の長さは 8 文字まで、大文字と小文字の区別は無い。 有効な文字はすべての英数字に加え、ダッシュ ('-') とアンダースコア ('_')を使用できる。"default"と いうユーザー名 は無効である。

Password - アカウントにオプションの新規または変更パスワードを入力する。 タイプした文字列は表示されず、アステリスク(*)のみ見える。パスワードは 8 文字までの英数字で大文字と小文字は区別される。

Confirm Password -パスワードを再入力して、正しく入力した ことを確認する。この欄は文字は表示せずアスタリスク(*)を示す。

Encryption Key - 暗号化プロトコル欄でDESを選択した場合、SNMPv3 暗号化 キーをここに入力する。 それ以外の場合この欄は無視される。 有効なキーは 8 から 64 文字までである。 暗号化プロトコルと暗号化キーを変更するためにはApplyチェックボックスをオンにする

構成不可能なデータ

Access Mode - ユーザーのアクセス･モードを示す。管理者アカウントは常時'Read･Write'アクセスであり、その他すべてのアカウントは'Read Only'の特権である。

SNMP v3 Access Mode - ユーザー･アカウントのSNMPv3 アクセス特権を示す。管理者アカウントは常時'Read･Write'アクセスであり、その他すべてのアカウントは'Read Only'の特権である。

コマンドボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても、新しい設定をスイッチ に保持させるには保存しなければなりません

Delete - 現在選択されているユーザー･アカウントを削除する。 スイッチにパワー･サイクル後、新 たな値を保持させるには、保存を実行しなければならない。.このボタンはユー ザーアカウントが「Read専用」アクセスの場合のみ表示されます。「Read/Write」ユーザーを削除できません。

8.2.5.2 認証リスト･コンフィグ

この画面からログイン･リストを構成できます。ログインリストは、リストに関連付けるユーザーに対してスイッチやポートアクセスを有効化するための認証モードを指定します。事前に構成されたユーザー、管理者、ゲストは削除不可の事前に構成されたデフォルトリストに割当てられます。新たに作成されたユーザーもすべて特に別のリストへ割当てる必要がなければデフォルトリストに割当てられます。

User Management

User Accounts | Authentication List Config | Authentication List Summary | User Login | Login Session

Authentication List: Create
Authentication List Name:*
* = mandatory
Apply

図 ： 認証リスト･コンフィグ

選択基準

Authentication List - 構成する認証ログイン･リストを選択する。 'Create/生成する'を 選択して新たなログイン･リストを定義する。新たなログイン･リストを生成する際、'ローカル'は初期認証方法として設定される。

Method 1 - 選択された認証ログイン･リストにまず表示される方法を選択する ためにこのドロップダウンメニューを使用する。'ローカル'等最初の方法としてタイムアウトしない方法を選ぶと、たとえ 1 個以上の方法を指定しても他の方法は試行されない。このパラメータはまず新たなログイン･リストを生成すると表示される。 オプション:

- **Local -** ローカルに保存されたユーザー名とパスワードが認証に使用される。
- **Radius -** ユーザー名とパスワードはローカルではなくRADIUSサーバにより認証される。
- **TACACS+ -**ユーザー名とパスワードはTACACS+サーバにより認証される。
- **LDAP-**ユーザー名とパスワードはLDAPサーバにより認証される。
- **Reject-** ユーザーは認証を常に拒否される。
- **Undefined -** 認証方法は未定である(この選択肢は最初の方法として割当てられない)。

Method 2 -選択された認証ログイン･リストに 2 番目に表示される方法ーこれがあ ればーを選択するためにこのドロップダウンメニューを使用する。これは最初の方法がタイムアウトした場合に使用される方法である。2 番目の方法としてタイムアウトしない方法を選択すると 3 番目の方法は試行されない。このパラメータはまず新たなログイン･リストを生成すると表示される。 t.

Method 3 -選択された認証ログイン･リストに 3 番目に表示される方法ーこれがあれば ーを選択するためにこのドロップダウンメニューを使用する。このパラメータはまず新たなログイン･リストを生成すると表示される。

構成可能データ

Authentication List Name - 新たなログイン･リストを生成する場合、割当てる 名前を入力する。 最大 15 文字の英数字であり、大文字と小文字を区別しないものとする。

コマンドボタン

Apply - 更新した画面をスイッチへ送り､スイッチでその変更が有効化される｡これ らの変更 は保存しなければ電源を切ると保持されません｡

Delete - 選択された認証リストを構成から削除する。 システム･ログインまたはIEEE 802.1xポ ート･アクセス制御で任意のユーザーに(デフォルト･ユーザーを含む)選択されたログイン･リストが割当てられると削除は失敗する。 このボタンはRead･Writeアクセス特権がある場合のみ使用できる。 当該変更は保存を実行しないとパワー･サイクル後、保持されない。

8.2.5.3 認証リスト･サマリ

User Management

User Accounts | Authentication List Config | Authentication List Summary | User Login | Login Session

Authentication List	Method List	Login Users	802.1x Port Security Users
defaultList	local	admin guest default	admin guest default

Refresh

図 : 認証リスト･サマリ

構成不可能なデータ

Authentication List - この行に一覧表示された認証ログイン･リストを識別する。

Method List - このログイン･リストに構成された方法の整理されたリスト。

Login Users - ユーザー･ログイン構成画面でこのログイン･ リストに割 当てた ユーザー。 このリストはシステム･ログイン ･アクセスでユーザーを認証するために使用される。

802.1x Port Security Users - ポート･アクセス制御 ユーザー ･ログ イン構成画面でこのログイン･リストに割当てるユーザーである。このリストはIEEE 802.1xプ ロ トコルに よりポート･アクセスを認証するために使用される。

コマンドボタン

Refresh - ページ情報を更新する。

8.2.5.4　**ユーザー･ログイン**

構成された各ユーザーはスイッチやスイッチのポートへアクセスしようとする際の認証方法が指定されたログインリストに割当てられます。ユーザーアカウント画面で新しいユーザーアカウントを作成後、この画面からそのユーザーをスイッチのログインリストに割当ててください。さらに必要に応じて、ポートアクセス制御のユーザーログイン構成画面でポートログインリストに割当てます。当該ユーザーに新たなログイン･リストを生成する必要があれば、認証リスト構成頁で行う。

初期設定ユーザーである管理者とゲストは削除できないデフォルト･リスト名の初期構成リストに割当てられている。すべての新たに生成されたユーザーも異なるリストに割当てるまではデフォルト･リストに割当てられる。

スイッチに構成されたアカウントを持たないユーザーは「デフォルト」または「未構成」ユーザーといっています。RADIUSサーバによる認証を指定ログインリストへ当該未構成ユーザーを割当てる場合、各スイッチのすべてのユーザーに対してアカウントを作る必要はありません。しかし、デフォルトの未構成ユーザーは「デフォルトリスト」に割当てずみであり、デフォルトではローカル認証を使用します。

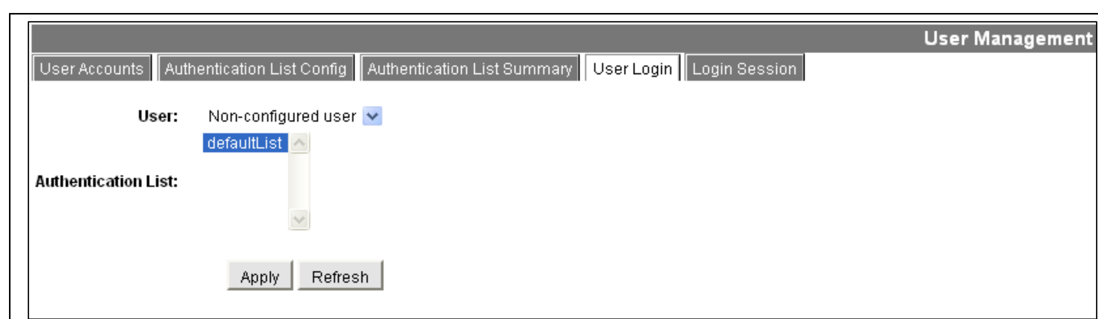


図　:ユーザー･アカウント･コンフィグ

選択基準

User - ログインリストに割当てるユーザーを選びます。管理者ユーザーはデフォ ルトリストに必ず関 連付けてください。これは強制的に管理者ユーザーを常にローカルで認証してスイッチ構成に全くアクセスできなくなることを防ぐためです。あるユーザーをリモート認証を要するログインリストに割当てる場合はすべてのCLI、ウェブ、Telnetセッションからスイッチへのアクセスは認証が完了 するまで遮断されます。RADIUS構成ヘルプ の最長遅延の説明を参照してください。

構成可能データ

Authentication List - システム･ログインでユーザーを割当てる認証ログイン･リストを選択する。

コマンドボタン

Apply - 更新した画面をスイッチへ送り、スイッチでその変更が有効化される。これらの変更は保存しなければ電源を切ると保持されません。

8.2.5.5 ログイン･セッション

この頁には、ユーザー名、接続元、アイドル･タイム、セッション･タイム、セッション･タイプからなるログイン･セッション情報が表示される。

User Management

User Accounts | Authentication List Config | Authentication List Summary | User Login | Login Session

ID	User Name	Connection From	Idle Time	Session Time	Session Type
00	admin	EIA-232	00:04:09	00:04:20	Serial Port
11	admin	192.168.2.188	00:00:00	00:03:57	HTTP

Refresh

図 : ログインセッション

構成不可能なデータ

ID -この行のIDを指す。

User Name - セッションを確立したユーザーの名前を示す。

Connection From - ユーザーがどのマシンから接続しているかを示す。

Idle Time - アイドル･セッション･タイムを示す。

Session Time - 合計セッション･タイムを示す。

Session Type - セッション･タイプを示す。: telnet、シリアルポート、SSH または HTTP.

コマンドボタン

Refresh - ページ情報を更新する。

8.2.6 ロギング

8.2.6.1 バッファー･ログを構成する

このログはメッセージの内容と重大度に基づいてメモリにメッセージを保存する。 スタック可能 システム上ではこのログはスタック･プラットフォームの最上部にのみ存在する。 スタックの他の プラットフォームはメッセージをスタック･ログの最上部に転送する。

Configuration
Buffered Log | Command Logger | Console Log | Hosts | Syslog
Admin Status: Enabled
Behavior: Wrap
Apply

図 :バッファー･ログ･コンフィグ

構成可能データ

Admin Status - "無効化"されているログはメッセージを記録しない。 "有効化"されて いるログがメッセージを記録する。ロギングの有効化と無効化はプルダウン入力欄の該当行を選択する。

Behavior ログ容量が最大になったときの動作を示す。 ログ容量が最大になると上書きするかしない。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。

8.2.6.2 コマンド･ロガーを構成する

Configuration
Buffered Log | Command Logger | Console Log | Hosts | Syslog
Admin Mode: Disabled
Apply

図 : コマンド･ロガー･コンフィグ

選択基準

Admin Mode - CLIコマンド･ロギングの有効化/無効化操作はプルダウンの 該当欄を選択 して、Applyをクリックする。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。

8.2.6.3 コンソール・ログを構成する

これはホストに接続されたどのシリアル機器にもメッセージのロギングを可能にする。

Configuration
Buffered Log | Command Logger | Console Log | Hosts | Syslog
Admin Status: Disabled
Severity Filter: Alert
Apply

図: コンソール・ログ・コンフィグ

選択基準

Admin Status - 「無効化」されたログはメッセージを記録しません。「有効化」された ログはメッセージを記録します。プルダウン入力欄から対応する行を選びログ機能を有効化/無効化します。

Severity Filter - ログは構成された閾値の重大性と同等かそれ以上のメッセージを記録します。プルダウン入力欄で対応する行を選び重大性のオプションを選択します。これら重大性のレベルを以下に列挙しました。

- Emergency (0): システムは使用不可
- Alert (1): 直ちにアクションを要する
- Critical (2): 致命的な状況
- Error (3): エラー状況
- Warning (4): 警戒を要する状況
- Notice(5): 通常ではあるが重要な状況
- Informational(6): 情報提供のみのメッセージ
- Debug(7): デバッグ・レベルのメッセージ

コマンドボタン

Apply - 入力した数値でスイッチを更新する。

8.2.6.4 **ホストを構成する**

ログ化メッセージをホストに送るように構成できる。

図: ロギング・ホスト・コンフィグ

選択基準

Host - シスログ用に構成されたホストのリストである。 構成を変更するホストを選択する、または、ドロップダウン・リストから新たなホストを追加する。

Severity Filter - ログは構成された重大度閾値に等しいまたはそれを超えるメッセージを記録する。 重大度オプションはプルダウン入力欄の該当行を選択して選択する。 これらの重大度レベルを次に列挙した：

- Emergency (0): システムは使用不可
- Alert (1): 直ちにアクションを要する
- Critical (2): 致命的な状況
- Error (3): エラー状況
- Warning (4): 警戒を要する状況
- Notice (5): 通常ではあるが重要な状況
- nformational (6): 情報提供のみのメッセージ
- Debug (7): デバッグ・レベルのメッセージ

構成可能データ

IP Address - シスログ用に構成されたホストのIPアドレスである。

Port - シスログ・メッセージが送られるホストのポートである。 デフォルト・ポートは514である。テキスト欄にポートを指定する。

構成不可能なデータ

Status - これはホストがアクティブにロギングするかを指定する。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。

Refresh - データベースを再取得して、テーブルの最初のエントリから始めて再表示する。

Delete - 構成されたホストを削除する。

8.2.6.5 **シスログを構成する**

システムでシスログ･システムを有効化するには、ログ化メッセージが"ホスト"頁で指定されたホストに送られる。

Configuration

Buffered Log | Command Logger | Console Log | Hosts | Syslog

Admin Status: Disable

Local UDP Port (1 to 65535) :* 514

Messages Received: 16

Messages Dropped: 0

Messages Relayed: 0

* = mandatory

Apply Refresh

図：シスログ･コンフィグ

選択基準

Admin Status - 構成されたシスログ･ホストへのロギングを有効化/無効化するためにある これを無効化するするとすべてのシスログ･ホストへのロギングを停止する。無効化とはここでどのコレクタ/リレーにもメッセージが送られないことを意味する。有効化とはコレクタ/リレー毎に構成された値で構成されたコレクタ/リレーにメッセージが送られることを意味する。シスログ機能の動作の有効化と無効化はプルダウン入力欄の該当行を選択する。

構成可能データ

Local UDP Port - シスログ･メッセージを送り出すローカル･ホストのポートである デフォルト･ポートは 514 である。テキスト欄にローカル･ポートを指定する。

構成不可能なデータ

Message Received - ログ･プロセスにより受信されたメッセージ数これには落とさ れたり無視され たメッセージも含む。

Message Dropped - エラーまたはリソース不足のあめプロセスできなかったメッセージ数

Message Relayed - シスログ機能によりシスログ･ホストへ転送たメッセージ数 複数のホストに転送されたメッセージはホスト毎に一回計数される。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。

Refresh- データベースを再取得し、テーブルの最初のエントリから改めて表示します。

8.2.6.6 **バッファー･ログを見る**

バッファー･ログ、持続的ログ、またはコンソール･ログに表示されたすべてのログ化メッセージの形式にメッセージを適用するのに役立つ。

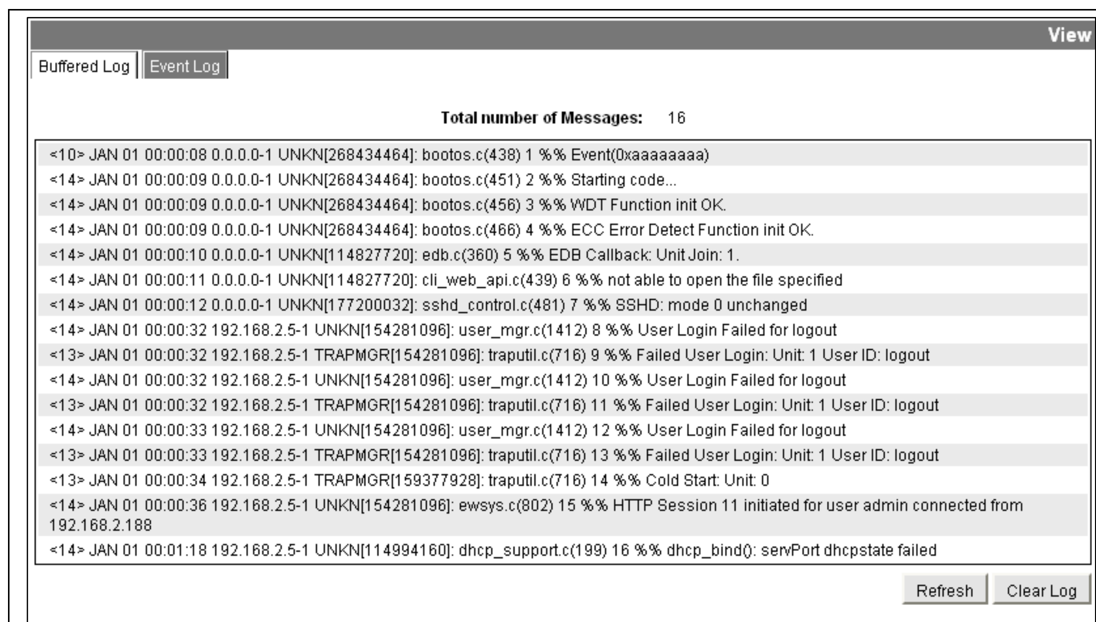


図 :バッファー･ログを見る

メッセージの形式

シスログを通してコレクタまたはリレーにログ化されたメッセージは同一形式である:

<15>Aug 24 05:34:05 0.0.0.0-1 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry (メッセージ･エイジ時間の終了にともないインタ ーフェイス 12 はルート･ステートに移行した)

- 上の例は､mstp_api.c ファイルの 318 行目によりスレッドID 2110 on Aug 24 05:34:05 で実行されていた MSTPコンポーネントにより作成されたシステムの重大性 7 (15mod8)(デバック) のメッセージを表し ています｡これはシステムIP 0.0.0.0 と ユニット番号 1 でログされた 237 番目のメッセージです｡

Total number of Messages: **バッファーされたログでは､最新の 128 項 目のみウェブペー ジに表示されます｡**

コマンドボタン

Refresh - **頁を最新ログ･エントリで更新する｡**

Clear Log - **ログ内すべてのエントリを消去する｡**

8.2.6.7　イベント･ログを見る

このパネルを使用してイベント･ログを表示する。破壊的イベント用エラー･メッセージを保持するために使用される。イベントが記録されフラッシュメモリに更新されたログが保存された後、スイッチはリセットされます。ログは最低でも 10080 のエントリを保持でき(実際の数字はプラットフォームとOSに依存しますが) フルになると項 目を追加しようとしても消去されます。イベントログはシステムがリセットされても保存 されます。

View

Buffered Log　Event Log

Entry		Filename	Line	TaskID	Code	Time
00001:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00002:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00003:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00004:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00005:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00006:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00007:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00008:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00009:	EVENT>	log_extend.c	732	09232D20	AAAAAAAA	1970/01/01 09:56:35

Refresh　Clear Log

図 : イベント･ログを見る

構成不可能なデータ

Entry -　イベント･ログ内のエントリ数 最新エントリが冒頭に来る。

Filename - イベントを検出したコードを識別するソース･コードのファイル名。

Line -　イベントを検出したコードのソース･ファイル内の行番号。

Task ID - イベントを報告するタスクのOSが割当てるID。

Code -　イベントを報告するコードによるイベント･ログ･ハンド ラに渡される イベント･コード。

Time -　直前リセット時点から起算したイベント発生時の時間。

コマンドボタン

Refresh - 頁を最新ログ･エントリで更新する。

Clear Log -　ログ内すべてのエントリを消去する。

8.2.7 統計

8.2.7.1 スイッチ・サマリ

Statistics

Switch Summary | Switch Detailed | Port Summary | Port Detailed

ifIndex:	49
Total Packets Received without Errors:	0
Broadcast Packets Received:	0
Packets Received with Errors:	0
Packets Transmitted without Errors:	2
Broadcast Packets Transmitted:	0
Transmit Packet Errors:	0
Address Entries Currently in Use:	1
VLAN Entries Currently in Use:	5
Time Since Counters Last Cleared:	0 day 0 hr 5 min 36 sec

Clear Counters | Refresh

図：IBP概観統計

構成不可能なデータ

ifIndex - このオブジェクトはこのスイッチのプロセッサと関連付けら れたインターフェイステー ブルのエントリインターフェイス番号を表示します。

Packets Received Without Errors - プロセッサに受信さ れたパケット総数 (ブロードキャスト・パケットとマルチキャスト・パケットを含む)

Broadcast Packets Received - ブロードキャス ト・アドレスにダイレクトされた受信パケット総数、 これにはマルチキャスト・パ ケットが 含まれないことに注意する。

Packets Received With Error - エラーが有るため高レイヤー・プロトコ ルに送信されなかったインバウンド・パケット数 **Packets Transmitted Without Errors -** インターフェイスから 送信されたパケット総数

Broadcast Packets Transmitted - 高レイヤー・プロト コルにブロードキャスト・アドレスへの送信を要求されたパケット総数で破棄されたものも送られなかったものも含む.**Transmit Packet Errors-** エラーのため送信できなかったアウト バウンド・パ ケット数

Address Entries Currently in Use -学習した静的エントリを含め スイッチで現在有効な転送データベースアドレステーブルのエントリの合計数。

VLAN Entries Currently in Use - VLANテーブルを 現在占有する VLANエントリ数

Time Since Counters Last Cleared - このスイッチ の統計が 最後にクリアされてからの日数、時間、分、秒表示の経過時間

コマンドボタン

Clear Counters - すべてのカウンターをクリアし、すべてのサマリをリセットし、詳細統計をデ フォルトに戻す。破棄されたパケットのカウント数はクリアできません。

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.2.7.2 スイッチの詳細

Statistics

Switch Summary | Switch Detailed | Port Summary | Port Detailed

ifIndex:	49
Octets Received:	0
Packets Received Without Error:	0
Unicast Packets Received:	0
Multicast Packets Received:	0
Broadcast Packets Received:	0
Receive Packets Discarded:	0
Octets Transmitted:	188
Packets Transmitted without Errors:	2
Unicast Packets Transmitted:	0
Multicast Packets Transmitted:	2
Broadcast Packets Transmitted:	0
Transmit Packets Discarded:	0
Most Address Entries Ever Used:	1
Address Entries in Use:	1
Maximum VLAN Entries:	3965
Most VLAN Entries Ever Used:	5
Static VLAN Entries:	5
Dynamic VLAN Entries:	0
VLAN Deletes:	0
Time Since Counters Last Cleared:	0 day 0 hr 5 min 54 sec

Clear Counters | Refresh

図:詳細な統計を切り換える

構成不可能なデータ

ifIndex - このオブジェクトはこのスイッチのプロセッサと関連付けられたインタ ーフェイステーブルのエントリインターフェイス番号を表示します。

Octets Received - プロセッサにより受信されたデータ・オクテット総数 (フレーム・ビットを除きFCSオクテットを含む)。

Packets Received Without Errors - プロセッサに受信された パケット総数 (ブロードキャスト・パケットとマルチキャスト・パケットを含む)

Unicast Packets Received - 高レイヤー・プロトコル にデリバリさ れたサブネットワーク・ユニキャスト・パケット数

Multicast Packets Received - マルチキャスト・アドレスにダイ レクトされた受信パケット総数 この総数にはブロードキ ャスト・アドレスにダイレクト されたパケットは含まれないことに注意する。

Broadcast Packets Received -ブロードキャスト・アドレ スにダイレクトさ れた受信パケット総数、これにはマルチキャスト・パケットが含まれない ことに注意する。

Receive Packets Discarded - 高レイヤー・プロトコルへの送信を妨げ るエラーが検出されなくても廃棄されたインバウンド・パケット数。 パケット廃棄の理由はバ ッファ ー容量を空けるためなど . **Octets Transmitted -** インターフェイスから送信された、 フレーム文字を含 むオクテット総数

Packets Transmitted Without Errors - インターフェイスから送信されたパケット総数

Unicast Packets Transmitted - 高レイヤー・プロトコルにサブ ネットワーク・ユニキャスト・アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む

Multicast Packets Transmitted -高レイヤー・プロトコルにマルチキャスト・アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む

Broadcast Packets Transmitted - 高レイヤー・プロトコルにブロードキャスト・アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む。

Transmit Packets Discarded - 高レイヤー・プロトコルへの送信を妨げるエラーが検出されなくても廃棄されたアウトバウンド・パケット数。 パケット廃棄の理由はバ ッファ ー容量を空けるためなど。

Most Address Entries Ever Used -再起動後にこの スイッチが学習した転送データベースアドレステーブルのエントリの最大数。

Address Entries in Use - このスイッチの転送データベースアドレステーブルの習得した、静的なエントリ数。

Maximum VLAN Entries -このスイッチに許可された仮想LAN(VLAN)の最大数

Most VLAN Entries Ever Used -最近の再起動以降このスイッチ上でアクティブであったVLANの最大数

Static VLAN Entries -静的に生成されたこのスイッチ上の現在アクティブなVLANエントリ数

Dynamic VLAN Entries - GVRP登録で生成されたこのスイッチ上の現在有効なVLANエントリの数 *(注記:この属性はファームウェアのスイッチ・モードで提供される)*

VLAN Deletes -最後の再起動以降に生成され削除されたこのスイッチ上の VLANの数**Time Since Counters Last Cleared -** このスイッチの統計が最後にクリアされて以降の日、時間、分、秒数の表示による経過時間。

コマンドボタン

Clear Counters - すべてのカウンターをクリアし、すべてのサマリをリセットし、詳しい統計値をデフォルトに戻す。破棄されたパケットのカウント数はクリアされません。

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.2.7.3 **ポート･サマリ**

Statistics

Switch Summary | Switch Detailed | Port Summary | Port Detailed

Slot/Port:	Encl-CB1/0/1
ifIndex:	1
Total Packets Received without Errors:	0
Packets Received with Errors:	0
Broadcast Packets Received:	0
Packets Transmitted without Errors:	0
Transmit Packet Errors:	0
Collision Frames:	0
Time Since Counters Last Cleared:	0 day 0 hr 6 min 6 sec

Clear Counters | Clear All Counters | Refresh

図 ： ポート･サマリ統計

選択基準

Slot/Port - データが表示されるまたは構成されるインターフェイスを選択する

構成不可能なデータ

ifIndex - アダプタ上でこのポートと関連付けられたインターフェイス･テーブル･エントリのインターフェイス番号を示すオブジェクトである。

Total Packets Received Without Errors- エラー無しで受信されたパケット総数

Packets Received With Errorト - エラーが有るため高レイヤー･プロトコルに送信されなかったインバウンド･パケット数Broadcast Packets Received - ブロードキャスト･アドレスにダイレクトされた正常な受信パケット総数 これにはマルチキャスト･パケットが含まれないことに注意する。

Packets Transmitted Without Errors - このポートによりセグメントへ送信されたフレーム数

Transmit Packet Errors - エラーのため送信できなかったアウトバウンド･パケット数

Collision Frames - 当該イーサネット･セグメントでのコリジョン総数

Time Since Counters Last Cleared - このポートの統計が最後にクリアされて以降経過した時間を日数、時間、分、秒までで示したもの。

コマンドボタン

Clear Counters - このポートのすべての統計をデフォルト値に戻す、すべてのカウンター消去

Clear All Counters - すべてのポートのすべての統計をデフォルト値に戻す、すべてのポート･カウンターの消去

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.2.7.4 **ポート詳細**

Statistics

Switch Summary | Switch Detailed | Port Summary | Port Detailed

Slot/Port:	Encl-CB1/0/1
ifIndex:	1
Packets RX and TX 64 Octets:	0
Packets RX and TX 65-127 Octets:	0
Packets RX and TX 128-255 Octets:	0
Packets RX and TX 256-511 Octets:	0
Packets RX and TX 512-1023 Octets:	0
Packets RX and TX 1024-1518 Octets:	0
Packets RX and TX 1519-2047 Octets:	0
Packets RX and TX 2048-4095 Octets:	0
Packets RX and TX 4096-9216 Octets:	0
Octets Received:	0
Packets Received 64 Octets:	0
Packets Received 65-127 Octets:	0
Packets Received 128-255 Octets:	0
Packets Received 256-511 Octets:	0
Packets Received 512-1023 Octets:	0
Packets Received 1024-1518 Octets:	0
Packets Received > 1522 Octets:	0
Total Packets Received without Errors:	0
Unicast Packets Received:	0
Multicast Packets Received:	0
Broadcast Packets Received:	0
Total Packets Received with MAC Errors:	0
Jabbers Received:	0
Undersize Received:	0
Fragments Received:	0
Alignment Errors:	0
Rx FCS Errors:	0
Overruns:	0

図：ポート詳細統計

選択基準

Slot/Port - データが表示されるまたは構成されるインターフェイスを選択する

構成不可能なデータ

ifIndex - アダプタ上でこのポートと関連付けられたインターフェイス･テーブル･エントリのインターフェイス番号を示すオブジェクトである。

Packets RX and TX 64 Octets - 長さ 64 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 65-127 Octets - 長さ 65 と 127 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 128-255 Octets - - 長さ 128 と 255 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 256-511 Octets -

長さ 256 と 511 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 512-1023 Octets -

長さ 512 と 1023 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 1024-1518 Octets -

長さ 1024 と 1518 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 1519-2047 Octets -

長さ 1519 と 2047 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 2048-4095 Octets -

長さ 2048 と 4095 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 4096-9216 Octets -

長さ 4096 と 9216 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Octets Received - ネットワークで受信された(失敗したパケットにあるものを含む)データ･オクテット総数 (フレーム･ビットを除きFCSオクテットを含む)。 このオブジェクトはイーサネット使用度の適度な推計値として使用できる。より高精度が必要な場合、etherStatsPktsとetherStatsOctetsオブジェクトが共通間隔の前後にサンプルされる必要がある。

Packets Received 64 Octets - 長さ 64 オクテットの受信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 65-127 Octets -長さ 65 と 127 オクテットの受信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 128-255 Octets -

長さ 128 と 255 オクテットの受信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 256-511 Octets -

長さ 256 と 511 オクテットの受信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 512-1023 Octets -

長さ 512 と 1023 オクテットの受信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 1024-1518 Octets -

長さ 1024 と 1518 オクテットの受信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received > 1522 Octets - 長さ 1522 オクテット以上の受信され(フレーム･ビットを除きFCSオクテットを含む).、良好に形成されたパケット総数(失敗したパケットを含む)。

Total Packets Received Without Errors - エラー無しで受信されたパケット総数。

Unicast Packets Received - 高レイヤー･プロトコルに送信されたサブネットワーク･ユニキャスト･パケット数。

Multicast Packets Received - マルチキャスト･アドレスにダイレクトされた正常な受信パケット総数 この総数にはブロードキャスト･アドレスにダイレクトされたパケットは含まれないことに注意する。

Broadcast Packets Received - ブロードキャスト･アドレスにダイレクトされた正常な受信パケット総数 これにはマルチキャスト･パケットが含まれないことに注意する。

Total Packets Received with MAC Errors - エラーが有るため高レイヤー･プロトコルに送信されなかったインバウンド･パケット総数

Jabbers Received - 長さ 1518 オクテット以上の受信され(フレーム･ビットを除きFCSオクテットを含む).、良好に形成され、さらにオクテットの整数倍による失敗したフレーム･チェック･シーケンス(FCSエラー)またはオクテットの非整数倍による失敗したFCS(アラインメント･エラー)があるパケット総数 このジャバー定義はIEEE-802.3 セクション 8.2.1.5 (10BASE5) とセクション 10.3.1.4 (10BASE2)の定義とは異なる。 この文書ではジャバーをパケットが 20msを超える条件として定義する。ジャバー検出許容範囲は 20msから 150msである。

Undersize Received - 64 オクテット未満の受信され(フレーム･ビットを除きFCSオクテットを含む).、良好なCRCによるパケット総数

Fragments Received - 64 オクテット未満の受信され(フレーム･ビットを除きFCSオクテットを含む).、CRCエラーがあるパケット総数

Alignment Errors - 長さ 64 オクテット以上 1518 オクテット以下の受信され(フレーム･ビットを除きFCSオクテットを含む).、 オクテットの非整数倍による失敗したフレーム･チェック･シーケンス (FCS) があるパケット総数

Rx FCS Errors - 長さ 64 オクテット以上 1518 オクテット以下の受信され(フレーム･ビットを除きFCSオクテットを含む).、 オクテットの整数倍による失敗したフレーム･チェック･シーケンス (FCS) があるパケット総数

Overruns - このポートが受信パケットにより過負荷状態となり、流入パケットに対応できなくなったために破棄されたフレーム総数

Total Packets Transmitted (Octets) - ネットワークで送信された(失敗したパケットにあるものを含む)データ･オクテット総数 (フレーム･ビットを除きFCSオクテットを含む). このオブジェクトはイーサネット使用度の適度な推計値として使用できる。 より高精度が必要な場合、etherStatsPktsとetherStatsOctetsオブジェクトが共通間隔の前後にサンプルされる必要がある。

PacketsTransmitted 64 Octets - 長さ 64 オクテットの受信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Transmitted 65-127 Octets -長さ 65 と 127 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 128-255 Octets --長さ 128 と 255 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 256-511 Octets -- 長さ 256 と 511 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 512-1023 Octets -長さ 512 と 1023 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 1024-1518 Octets - 長さ 1024 と 1518 オクテットの受信または送信された(フレーム･ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Maximum Frame Size - イーサネット･ヘッダー、CRC、ペイロードを含みインターフェイスがサポートするまたは構成された最大イーサネット･フレーム･サイズ --> (1518 ‐ 9216). デフォルト最大フレーム･サイズは 1518 である。

Total Packets Transmitted Successfully - インターフェイスから送信されたパケット総数。

Unicast Packets Transmitted -高レイヤー･プロトコルにサブネットワーク･ユニキャスト･アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む。

Multicast Packets Transmitted-高レイヤー･プロトコルにマルチキャスト･アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む。

Broadcast Packets Transmitted - 高レイヤー･プロトコルにブロードキャスト･アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む。

Total Transmit Errors - シングル、マルチ、エクセシブ･コリジョンの合計値

Tx FCS Errors- 長さ 64 オクテット以上 1518 オクテット以下の送信され(フレーム・ビットを除きFCSオクテットを含む)。、 オクテットの整数倍による失敗したフレーム・チェック・シーケンス (FCS) があるパケット総数。

Underrun Errors - 送信FIFOバッファーがフレーム送信中に空になったため破棄されたフレーム総数

Total Transmit Packets Discarded - 破棄されたシングル・コリジョン・フレーム、破棄されたマルチ・コリジョン・フレーム、破棄されたエクセシブ・フレームの合計値。

Single Collision Frames - 送信がコリジョン 1 回のみ妨害された特定インターフェイス上で送信が完了したフレーム数。

Multiple Collision Frames - 送信が 1 回以上のコリジョンで妨害された特定インターフェイス上で送信が完了したフレーム数。

Excessive Collision Frames - 過度のコリジョンにより特定インターフェイスでの送信障害を起こしたフレーム数

GVRP PDUs Received – GARPレイヤーで受信したGVRP PDUのカウント

GVRP PDUs Transmitted – GARPレイヤーから送信されたGVRP PDUのカウント

GVRP Failed Registrations – GVRPの登録を試みて完了できなかった回数

GMRP PDUs Received – GARPレイヤーから受信したGMRP PDUのカウント

GMRP PDUs Transmitted – GARPレイヤーから送信されたGMRP PDUのカウント

GMRP Failed Registrations – GMRP登録を試みたが完了できなかった回数

STP BPDUs Received – 選択したポートで受信したSTP BPDUの数

STP BPDUs Transmitted – 選択したポートから送信したSTP BPDUの数

RSTP BPDUs Received – 選択したポートで受信したRSTP BPDUの数

RSTP BPDUs Transmitted – 選択したポートから送信したRSTP BPDUの数

MSTP BPDUs Received – 選択したポートで受信したMSTP BPDUの数

MSTP BPDUs Transmitted – 選択したポートから送信したMSTP BPDUの数

Time Since Counters Last Cleared - このポートこのポート の統計が最後にクリアされて以降経過した時間を日数、時間、分、秒までで示したもの。

コマンドボタン

Clear Counters - このポートのすべての統計をデフォルト値に戻す、すべてのカウンター消去

Clear All Counters/すべてのカウンターをクリアする - すべてのポートのすべてのカウンターをクリアし、すべてのポートの統計をリセットしてデフォルト値に戻す。

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.2.8 SNMP

8.2.8.1 コミュニティー・コンフィグ

デフォルトでは 2 個のSNMPコミュニティーがある：

– プライベート。'Read・Write'特権とステータスが有効化に設定されている。

– パブリック。'Read Only'特権とステータスが有効化に設定されている。

これらは周知のコミュニティーです、このメニューによりデフォルトを変更するか、他のコミュニティーを追加します。このメニューにより定義するコミュニティーのみがSNMPv1 とSNMPv2cのプロトコルによりスイッチへアクセスできます。Read/WriteレベルのアクセスができるコミュニティのみがSNMP経由のこのメニューへアクセスできます。

SNMPv1 とSNMPv2cプロトコルを使用するときはこのメニューを使用しなければならない。 SNMP v3 を使用する場合、ユーザー・アカウント・メニューを使用する。

SNMP

Community Config | Trap Receiver Config | Trap Flags | Trap Log | Supported MIBs

Community: public
SNMP Community Name:* public
Client IP Address:* 0 . 0 . 0 . 0
Client IP Mask:* 0 . 0 . 0 . 0
Access Mode: Read Only
Status: Enable

* = mandatory

Apply Delete

SNMP Community Name	Client IP Address	Client IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read Only	Enable
private	0.0.0.0	0.0.0.0	Read/Write	Enable

図: SNMPコミュニティー構成

選択基準

Community - 既存コミュニティーを再構成する、または新たなアカウントを生成するにはこの画面を使用できる。このプルダウン・メニューから既存コミュニティーの名前を選択する、または'Create'を選択して新たなコミュニティーを追加できる。

Access Mode - プルダウン・メニューからRead・WriteまたはRead Onlyを選択してこのコミュニティーのアクセスレベルを指定する

Status - プルダウン・メニューから有効化または無効化を選択してこのコミュニティーのステータスを指定する 有効化を選択すると、コミュニティー名はすべての有効なコミュニティー名に固有でなければならない。さもないと設定要求は拒否される。 無効化を選択すると、コミュニティー名は無効化される。

構成可能データ

SNMP Community Name - SNMPコミュニティー名であり、SNMPコミュニティー間を識別する。 SNMPコミュニティー内のコミュニティー名は固有でなければならない。有効な入力は最大 16 文字までの大文字と小文字が区別される文字列である。

Client IP Address - クライアントIPアドレスとクライアントIPマスクはまとめて見ると、そこからSNMPクライアントが当該コミュニティーを使用してこの装置にアクセスできるIPアドレスの範囲を指す。IPアドレスまたはIPマスクの値が

0.0.0.0 の場合、任意のIPアドレスからアクセスできる。それ以外の場合、各クライアントのIPアドレスはクライアントIPアドレスがそうであるように、マスクと結合され、また、各値が等しい場合、アクセスは許可される。たとえば、クライアントIPアドレスとクライアントIPマスク・パラメータが 192.168.1.0/255.255.255.0 の場合、IPアドレスが 192.168.1.0 から 192.168.1.255 までのどのクライアントからでもアクセスできる。1 台のみのワークステーションからアクセスを許可する場合、クライアントIPマスク値を 255.255.255.25 とし、当該マシンのIPアドレスをクライアントIPアドレスに使用する。

Client IP Mask - クライアントIPアドレスとクライアントIPマスクはまとめて見ると、そこからSNMPクライアントが当該コミュニティーを使用してこの装置にアクセスできるIPアドレスの範囲を指す。IPアドレスまたはIPマスクの値が 0.0.0.0 の場合、任意のIPアドレスからアクセスできる。それ以外の場合、各クライアントのIPアドレスはクライアントIPアドレスがそうであるように、マスクと結合され、また、各値が等しい場合、アクセスは許可される。たとえば、クライアントIPアドレスとクライアントIPマスク・パラメータが 192.168.1.0/255.255.255.0 の場合、IPアドレスが 192.168.1.0 から 192.168.1.255 までのどのクライアントからでもアクセスできる。1 台のみのワークステーションからアクセスを許可する場合、クライアントIPマスク値を 255.255.255.25 とし、当該マシンのIPアドレスをクライアントIPアドレスに使用する。

コマンドボタン

Apply - 画面の設定をスイッチに更新する。電源を切っても新しい設定をスイッチに保持させるには保存しなければなりません

Delete - 現在選択されているコミュニティー名を削除します。電源を切っても新しい設定をスイッチに保持させるには保存しなければなりません。

8.2.8.2 トラップ･レシーバー･コンフィグ

このメニューはアクティブなトラップ･レシーバー毎にエントリを表示する。

SNMP
Community Config | Trap Receiver Config | Trap Flags | Trap Log | Supported MIBs
Community: Create
SNMP Community Name:*
SNMP Version: SNMP v2
IP Address:* 0 . 0 . 0 . 0
Status: Disable
* = mandatory
Apply

図 ：SNMP トラップ･レシーバー･コンフィグ

選択基準

Community - 既存コミュニティーを再構成する、または新たなアカウントを生成するにはこの画面を使用できる。このプルダウン･メニューから既存コミュニティーの名前を選択する、または'Create'を選択して新たなコミュニティーを追加できる。

SNMP Version - プルダウン･メニューからレシーバーが使用するトラップ･バージョンを選択する：

– SNMP v1 - SNMP v1 を使用してトラップをレシーバーに送る

– SNMP v2 - SNMP v2 を使用してトラップをレシーバーに送る

ステータス - プルダウン･メニューからレシーバーのステータスを選択する：

– 有効化 - トラップをレシーバーに送る

– 無効化 - トラップをレシーバーに送らない

構成可能データ

SNMP Community Name - SNMPトラップ･パケットがトラップ･マネージャに送られるようにコミュニティー文字列を入力する 最大 16 文字で大文字と小文字は区別される。

IP Address - この装置からSNMPトラップを受信するIPアドレスを入力する。 0 から 255 までの 4 個の数字をピリオドで区切り入力する。

コマンドボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても、新しい設定をスイッチ に保持させるには保存しなければなりません

Delete - 現在選択されているコミュニティー名を削除します。電源を切っても新しい設定をスイッチに保持させるには保存しなければなりません。

8.2.8.3　トラップ･フラッグ

このメニューにより有効化するトラップを指定します。アクティブなトラップに識別される条件にスイッチが合致すると、トラップメッセージが任意の有効化されたSNMPトラップレシーバーへ送られメッセージがトラップログに書かれます。

図 ：SNMPトラップ･フラッグ

選択基準

Authentication - プルダウン入力欄の対応行を選択して認証失敗トラップを有効化または無効化する。 デフォルト設定は有効化されている。

Link Up/Down - プルダウン入力欄の対応行を選択してリンク･ステータス･トラップを有効化または無効化する。デフォルト設定は有効化されている。

Multiple Users - プルダウン入力欄の対応行を選択して複数ユーザー･トラップを有効化または無効化する。 デフォルト設定は有効化されている。このトラップは同じユーザーIDが同時に一回以上スイッチへログイン(Telnet またはシリアルポート経由で)したときに実施されます。

Spanning Tree － プルダウン入力欄の対応する行を選んでスパニング ツリートラップの機能を有効化または無効化する。工場出荷時デフォルトでは有効化されています。

ACL Traps - プルダウン入力欄の対応行を選択してACLトラップを有効化または無効化する 工場側デフォルトは無効化されている。

コマンドボタン

Apply - 更新した画面をスイッチへ送りスイッチ上で変更を有効化する。保存しなければ電源を切っても変更は保持されません。

8.2.8.4 トラップ·ログ

この画面はトラップログのエントリをリストします。この情報はシステムユーティリティーの「スイッチからファイルをアップロードする」によりファイルとして受信されます。

SNMP

Community Config | Trap Receiver Config | Trap Flags | Trap Log | Supported MIBs

Number of Traps Since Last Reset: 4
Trap Log Capacity: 256
Number of Traps Since Log Last Viewed: 4

Log	System Up Time	Trap
0	1970/01/01 08:00:34	Cold Start: Unit: 0
1	1970/01/01 08:00:33	Failed User Login: Unit: 1 User ID: logout
2	1970/01/01 08:00:32	Failed User Login: Unit: 1 User ID: logout
3	1970/01/01 08:00:32	Failed User Login: Unit: 1 User ID: logout

Clear Log

図 :SNMPトラップ·ログ

構成不可能なデータ

Number of Traps Since Last Reset - 直前にトラップ·ログ·エントリが生成されてから生成されたトラップ数。

Trap Log Capacity - ログに保存されるトラップの最大数 この容量をトラップ数が超過すると、エントリは古いエントリ順に上書きする。

Number of Traps since log last viewed – トラップが最後に表示されて以降発生したトラップの数。どんな方法(ターミナルインターフェイス表示、ウェブ表示、スイッチからファイルのアップロード等)でトラップを表示してもこのカウンターはゼロへクリアされます。

Log - このトラップのシーケンス番号

System Up Time - 最後の再起動以降このトラップが発生した日時を日、時間、分、秒で表示する。

Trap - トラップの識別情報

コマンドボタン

Clear Log - ログ内すべてのエントリを消去する。 この後にログを表示すると新たなログ·エントリのみ表示される。

8.2.8.5　サポートされるMIB

これはスイッチにサポートされているすべてのMIBのリストです。

SNMP

Community Config | Trap Receiver Config | Trap Flags | Trap Log | Supported MIBs

Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB	Remote Network Monitoring Management Information Base
FSC-SWITCH-MIB	Fujitsu Siemens Computers Reference
SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
SNMP-FRAMEWORK-MIB	The SNMP Management Architecture MIB
SNMP-MPD-MIB	The MIB for Message Processing and Dispatching
SNMP-NOTIFICATION-MIB	The Notification MIB Module
SNMP-TARGET-MIB	The Target MIB Module
SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-based Security Model.
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.
USM-TARGET-TAG-MIB	SNMP Research, Inc.
LAG-MIB	The Link Aggregation module for managing IEEE 802.3ad
RFC 1213 - RFC1213-MIB	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1493 - BRIDGE-MIB	Definitions of Managed Objects for Bridges (dot1d)
RFC 2674 - P-BRIDGE-MIB	The Bridge MIB Extension module for managing Priority and Multicast Filtering, defined by IEEE 802.1D-1998.
RFC 2674 - Q-BRIDGE-MIB	The VLAN Bridge MIB module for managing Virtual Bridged Local Area Networks
RFC 2737 - ENTITY-MIB	Entity MIB (Version 2)
RFC 2863 - IF-MIB	The Interfaces Group MIB using SMIv2
RFC 3635 - Etherlike-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types
SWITCHING-MIB	Switching - Layer 2
SWITCHING-EXTENSION-MIB	Switching extension - Layer 2
INVENTORY-MIB	Unit and Slot configuration.
PORTSECURITY-PRIVATE-MIB	Port Security MIB.
IEEE8021-PAE-MIB	Port Access Entity module for managing IEEE 802.1X.
TACACS-MIB	TACACS MIB
RADIUS-CLIENT-PRIVATE-MIB	Radius MIB
RADIUS-ACC-CLIENT-MIB	RADIUS Accounting Client MIB

図：SNMPがサポートするMIB

構成不可能なデータ

Name - 該当する場合はRFC番号、およびMIB名

Description - RFCの表題またはMIBの内容

コマンドボタン

Refresh - データを更新する

8.2.9 SNTP

8.2.9.1 グローバル･コンフィグ

SNTP
Global Config | Global Status | Server Config | Server Status | Current Time | Time Zone Settings

Client Mode: Disable
Port (1 to 65535):* 123
Unicast Poll Interval (6 to 10,which mean 2^6 to 2^10 in sec.):* 6
Broadcast Poll Interval (6 to 10,which mean 2^6 to 2^10 in sec.):* 6
Unicast Poll Timeout (1 to 30):* 5
Unicast Poll Retry (0 to 10):* 1

* = mandatory

Apply

図 : SNTP グローバル･コンフィグ

選択基準

Client Mode - SNTPクライアントの動作モードを指定する SNTPクライアントは次のモードのいずれかで動作する。デフォルト値は"無効化"である。

- ***Disable***- SNTPは動作しない クライアントからSNTP要求が送信されなかった、または、受信されたSNTPメッセージが処理されなかった。
- ***Unicast***- SNTPは 2 点間で動作する ユニキャスト･クライアントはユニキャスト･アドレスで指定サーバに要求を送り、応答を予期する、この応答によりクライアントは時間を決定し、オプションとしてはサーバとの往復遅延時間とローカル･クロックのオフセットを決めることができる。
- ***Broadcast*** - SNTP はマルチキャスト･モードと同じ動作をするが、マルチキャスト･アドレスではなくローカルのブロードキャスト･アドレスを使用する。 ブロードキャスト･アドレスは 1 個のサブネット･スコープを持つが、マルチキャスト･アドレスはインターネット全体のスコープがある。

構成可能データ

Port - 応答/ブロードキャストを聞くローカルUDP ポートを指定する 許可範囲は 1 から 65,535 である。 デフォルト値は 123 である。

Unicast Poll Interval - ユニキャスト･モードに構成された場合 2 の倍数である、ユニキャスト･ポル要求間隔秒数を指定する 許可範囲は 6 から 10 である。 デフォルト値は 6 である。

Broadcast Poll Interval - ブロードキャスト･モードに構成された場合 2 の倍数で表現される、ブロードキャスト･ポル要求間隔秒数を指定する この間隔が経過する前に受信されたブロードキャストは破棄される。 許可範囲は 6 から 10 である。 デフォルト値は 6 である。

Unicast Poll Timeout - ユニキャスト･モードに構成された場合SNTP応答までの待機秒数を指定する 許可範囲は 1 から 30 である。 デフォルト値は 5 である。

Unicast Poll Retry - ユニキャスト･モードに構成された場合次の構成されたサーバの使用を試行するまでに、最初のタイムアウトからSNTPサーバに要求を再試行する回数を指定する 許可範囲は 0 から 10 である。 デフォルト値は 1 である。

コマンドボタン

Apply - 更新した構成をスイッチへ送る。構成の変更は即時に有効化されます。

8.2.9.2 グローバル・ステータス

SNTP

Global Config | Global Status | Server Config | Server Status | Current Time | Time Zone Settings

Version:	4
Supported Mode:	Unicast & Broadcast
Last Update Time:	JAN 01 00:00:00 1970
Last Attempt Time:	JAN 01 00:00:00 1970
Last Attempt Status:	Other
Server IP Address:	
Address Type:	Unknown
Server Stratum:	0 - Unspecified
Reference Clock Id:	
Server Mode:	Reserved
Unicast Server Max Entries:	3
Unicast Server Current Entries:	0
Broadcast Count:	0

図：SNTP グローバル・ステータス

構成不可能なデータ

Version - クライアントがサポートするSNTPバージョンを指定する。

Supported Mode - クライアントがサポートするSNTPモードを指定する。 複数のモードをクライアントがサポートできる。

Last Update Time - SNTPクライアントが最後にシステム・クロックを更新したローカル日付時刻（UTC）を指定する。

Last Attempt Time - 直前のSNTP要求または要求しなかったメッセージの受信時であるローカル日付時刻（UTC）を指定する。

Last Attempt Status - ユニキャストとブロードキャスト・モードに対して直前のSNTP要求または要求しなかったメッセージのステータスを指定する。 サーバからメッセージが受信されない場合、Otherのステータスが表示される。 これらの値はすべての動作モードに適格である。

- ***Other*** - 次の列挙値のいずれでもない場合。
- ***Success*** - SNTP動作は成功した、システム時間は更新された。
- ***Request Timed Out*** - SNTPサーバから応答を受信しないダイレクトされたSNTP要求タイムアウト。
- ***Bad Date Encoded*** - SNTPサーバによる時間が有効ではない。
- ***Version Not Supported*** – サーバがサポートするSNTPバージョンはクライアントがサポートするバージョンと互換性が無い。
- ***Server Unsynchronized*** - SNTPサーバがピアと同期化されていない。 これはSNTPメッセージの'leap indicator' 欄に表示される。
- ***Server Kiss Of Death*** - SNTPサーバがこのサーバにはクエリーを送信止めるよう指示した。 これはサーバから受けたメッセージで層欄が 0 であることにより示される。

Server IP Address - 直前に受信された有効なパケットにサーバのIPアドレスを指定する。 どのサーバからもメッセージが受信されなかった場合、空白が表示される。

Address Type - 直前に受信された有効なパケットについてSNTPサーバのアドレス・タイプを指定する。

Server Stratum - 直前に受信された有効なパケットについてサーバの要求層を指定する。

Reference Clock Id - 直前に受信された有効なパケットについてサーバの参照クロック識別子を指定する。

Server Mode - 直前に受信された有効なパケットについてサーバのモードを指定する。

Unicast Sever Max Entries - このクライアントに構成可能なユニキャスト・サーバ・エントリの最大数を指定する。

Unicast Server Current Entries - このクライアントに構成された現在のユニキャスト・サーバ・エントリ数を指定する。

Broadcast Count - 直前の再起動以降SNTPクライアントにより受信され処理された要求しなかったブロードキャストSNTPメッセージ数を指定する。

8.2.9.3 サーバ･コンフィグ

SNTP

Global Config | Global Status | Server Config | Server Status | Current Time | Time Zone Settings

Server: Create

IP Address

Port (1 to 65535):* 123

Priority (1 to 3):* 1

Version (1 to 4):* 4

* = mandatory

Apply Delete

図 :SNTPサーバ･コンフィグ

選択基準

Server - 追加の"Create".オプション付きで既存のサーバ･アドレスをすべて指定する "Create"を選択すると別のテキストボックス"Address"が表示され、ここには構成するサーバのアドレスを入力できる。

Address Type - 構成されたSNTPサーバ･アドレスのアドレス･タイプを指定する 許可されるタイプ：

– IPv4:

– ホスト名

デフォルト値はIPV4 である。

構成可能データ

Address - SNTPサーバ･アドレスを指定する これはSNTPサーバのエンコード化ユニキャストIPアドレスかホスト名を含む最大 64 文字の文字列である。 ユニキャストSNTP要求はこのアドレスに送られる。 このアドレスがDNSホスト名である場合、そのホスト名はSNTP要求が送信される毎にIPアドレスに解決される必要がある。

Port - SNTP要求が送信されるサーバのポートを指定する 許可範囲は 1 から 65,535 である。 デフォルト値は 123 である。

Priority - SNTP要求が送られるサーバ･シーケンスを決めるこのサーバ･エントリのプライオリティを指定する クライアントは応答受信に成功するかすべてのサーバに要求を処理させるまでは異なるサーバに要求を送り続ける。 このオブジェクトはサーバ･クエリーを行う順番を示す。 プレシデンスが 1 のサーバ･エントリはプライオリティが 2 等のサーバより先にクエリーを行われる。 1 個以上のサーバが同じプライオリティを持つ場合、要求順序はこのテーブルにあるエントリの辞書的順序に従う。 許可範囲は 1 から 3 である。 デフォルト値は 1 である。

Version - サーバで実行されるNTPバージョンを指定する 許可範囲は 1 から 4 である。 デフォルト値は 4 である。

コマンドボタン

Apply - 更新した構成をスイッチへ送る。構成の変更は即時に有効化されます。

Delete - SNTPサーバのエントリを削除する。更新した構成をスイッチへ送る。構成の変更は即時に有効化されます。

8.2.9.4 サーバ･ステータス

SNTP

Global Config | Global Status | Server Config | Server Status | Current Time | Time Zone Settings

Address:	1.2.3.4
Last Update Time:	
Last Attempt Time:	JAN 01 00:00:00 1970
Last Attempt Status:	Other
Unicast Server Num Requests:	0
Unicast Server Num Failed Requests:	0

図 : SNTP サーバ･ステータス

構成不可能なデータ

Address- 既存のすべてのサーバ･アドレスを指定する サーバ構成が存在しない場合、"No SNTP server exists" メッセージが画面に点滅する。

Last Update Time - 最後にシステム･クロックの更新にこのサーバからの応答が使用されたローカル日付時刻 (UTC) を指定する。

Last Attempt Time - このSNTPサーバが直前にクエリーされたローカル日付時刻(UTC) を指定する。

Last Attempt Status - このサーバへのSNTP要求ステータスを指定する。 このサーバからパケットが受信されない場合、Otherのステータスが表示される。

- ***Other*** - 次の列挙値のいずれでもない場合。
- ***Success*** - SNTP動作は成功した、システム時間は更新された。
- ***Request Timed Out*** - SNTPサーバから応答を受信しないダイレクトされたSNTP要求タイムアウト。
- ***Bad Date Encoded*** - SNTPサーバによる時間が有効ではない。
- ***Version Not Supported*** – サーバがサポートするSNTPバージョンはクライアントがサポートするバージョンと互換性が無い。
- ***Server Unsynchronized*** - SNTPサーバがピアと同期化されていない。 これはSNTPメッセージの'leap indicator' 欄に表示される。
- ***Server Kiss Of Death*** - SNTPサーバがこのサーバにはクエリーを送信止めるよう指示した。 これはサーバから受けたメッセージで層欄が 0 であることにより示される。

Unicast Server Num Requests - 最後のエージェント再起動以降このサーバに対して行われたSNTP要求回数をを指定する。

Unicast Server Num Failed Requests - 最後のエージェント再起動以降のサーバに対して行われたSNTP要求の失敗回数をを指定する

8.2.9.5 現在時刻

SNTP
Global Config | Global Status | Server Config | Server Status | Current Time | Time Zone Settings
Year (2000 - 2099):* 1970
Month (1 - 12):* 1
Day (1 - 31):* 1
Hour (0 - 23):* 8
Minute (0 - 59):* 8
Second (0 - 59):* 42
* = mandatory
Apply

図：SNTP現在時刻

構成可能データ

Year　年(4 桁). (範囲: 2000 – 2099).

Month – Month. (範囲: 1 – 12).

Day – 月の日 (範囲: 1 – 31).

Hour – 24 時間形式の時間.(範囲: 0 – 23).

Minute – Minute. (範囲: 0 – 59).

Second – Second. (範囲: 0 – 59).

コマンドボタン

Apply – 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければパワーサイクルでは保持されません。

8.2.9.6 **時間帯設定**

SNTPはタイムサーバからの定期的更新に基づく内部クロックをスイッチが設定できるようにしています。スイッチでの正確な時間を維持することはシステムがイベントエントリの有意な日付と時間を記録することを可能にしています。CLIにより手動でクロックを設定することもできます。クロックが設定されていなければスイッチは最後の起動で設定された工場出荷時デフォルトの時間のみを記録します。

SNTP	
Global Config / Global Status / Server Config / Server Status / Current Time / Time Zone Settings	
Time Zone Name:*	Taipei
Time Zone Hours (0 - 12):*	8
Time Zone Minutes (0 - 59):*	0
Direction:	Before UTC
* = mandatory	
	Apply

図：SNTP時間帯設定

選択基準

Direction

- before-utc - ローカル時間帯を UTCより先(東側)に設定する。
- after-utc - ローカル時間帯を UTCより後(西側)に設定する。

構成可能データ

Time Zone Name - 時間帯名、通常は略語を用いる (範囲: 1-15 文字).

Time Zone Hours - UTC前後の時間数 (範囲: 0～12 時間).

Time Zone Minutes - UTC前後の分数 (範囲: 0～59 分).

コマンドボタン

Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければ電力サイクルでは保持されません。

8.2.10 CDP

8.2.10.1 構成

このメニューによりCDPのためのパラメータを構成します、それがLAN内でのCISCOデバイスを発見するために使われます。

CDP

Config | Neighbor Info | Statistic

Admin Mode: Enable

Hold Time (10 - 255)Sec:* 180

Transmit Interval (5 - 254)Sec:* 60

Slot/Port	
All	
Encl-CB1/0/1	Enable
Encl-CB1/0/2	Enable
Encl-CB1/0/3	Enable
Encl-CB1/0/4	Enable
Encl-CB1/0/5	Enable
Encl-CB1/0/6	Enable
Encl-CB1/0/7	Enable
Encl-CB1/0/8	Enable
Encl-CB1/0/9	Enable
Encl-CB1/0/10	Enable
Encl-CB1/0/11	Enable
Encl-CB1/0/12	Enable
Encl-CB1/0/13	Enable
Encl-CB1/0/14	Enable
Encl-CB1/0/15	Enable
Encl-CB1/0/16	Enable
Encl-CB1/0/17	Enable
Encl-CB1/0/18	Enable
Encl-CB1/0/19	Enable
Encl-CB1/0/20	Enable
Encl-CB1/0/21	Enable
Encl-CB1/0/22	Enable

図: CDP 構成

選択基準

Admin Mode - CDP管理者モードを有効化または無効化する

Port State - すべてのポートのCDP管理者モードを有効化または無効化する

構成可能データ

Hold Time - 受信したCDPパケットの合法的な期間

Transmit Interval - CDPパケットを送る間隔

構成不可能なデータ

Slot/Port - ポートのリストを指定します

コマンドボタン

Apply - 更新した画面をスイッチへ送りスイッチ上で変更を有効化する。保存しなければ電源を切ると変更は保持されません。

8.2.10.2 周辺情報

CDP

Config | Neighbor Info | Statistic

Capability Codes : R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID	Intf	Time	Capability	Platform	Port ID

Clear Refresh

図: CDP 周辺情報

構成不可能なデータ

Device ID – 文字列の形式でデバイス名を識別します

Intf– CDPの周辺情報を受信するポート

Time – デバイスがCDP情報を保持すべき時間。

Capability – デバイスタイプ、たとえばスイッチ等の形式を表示します**Platform/プラットフォーム** – たとえばFSC L2ネットワークスイッチのようなデバイスのハードウェアプラットフォーム名を解説します

Port ID – CDPパケットが送られるポートを識別します

コマンドボタン

Clear - すべてのカウンターをクリアし、すべてのサマリをリセットし、詳しい統計値をデ フォルトに戻す。破棄されたパケットのカウント数はクリアされません。

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.2.10.3 統計

このメニューを使いCDPトラフィックの統計を表示する



図: CDP 統計

構成不可能なデータ

Incoming Packet Number – 周辺から受信する正常なCDPパケットの数

Outgoing Packet Number – このデバイスから送信したCDPパケットの数

Error Packet Number – 周辺から受信した違法なCDPパケットの数

コマンドボタン

Clear Counters - すべてのカウンターをクリアし、すべてのサマリをリセットし、詳しい統計値をデフォルトに戻す。破棄されたパケットのカウント数はクリアされません。

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.2.11　LDP

8.2.11.1　グローバル･コンフィグ

Configuration

Global Config　Interface Config

Transmit Interval (1 to 32768) :* 30

Hold Multiplier (2 to 10) :* 4

Re- Initialization Delay (1 to 10) :* 2

Notification Interval (5 to 3600) :* 5

* = mandatory

Apply

図：LLDP　グローバル･コンフィグ

構成可能データ

Transmit Interval - LLDPフレームの送信間隔を秒単位で指定する。範囲は 1 から 32768 である。 デフォルト値は 30 秒である。

Hold Multiplier - TTLを割当てる送信間隔に適用される乗数を指定する。 範囲は 2 から 10 である。デフォルト値は 4 である。

Re-Initialization Delay - 再初期化までの遅延時間を指定する。 . 範囲は 1 から 10 である。デフォルト値は 2 秒である。

Notification Interval - 通知の送信間隔を秒数で指定する。範囲は 5 から 3600 である。デフォルト値は 5 秒である。

コマンドボタン

Apply - 更新した画面をスイッチへ送ります。 変更はスイッチ上で有効化されますが保存しなければこれらの変更は電源を切ると保持されません。

8.2.11.2 インターフェイス･コンフィグ

Configuration
Global Config | Interface Config
Interface: All
Transmit: Disable
Receive: Disable
Notify: Disable
Transmit Management Information:
Optional TLV(s): System Name
System Description
System Capabilities
Port Description
Apply

図：LLDP インターフェイス･コンフィグ

選択基準

Interface -LLDP - 802.1ABを構成できるポートのリストを指定する。

Transmit - 選択されたインターフェイスにLLDP - 802.1ABの送信モードを指定する。

Receive - 選択されたインターフェイスにLLDP - 802.1ABの受信モードを指定する。

Notify - 選択されたインターフェイスにLLDP - 802.1ABの通知モードを指定する。

構成可能データ

Transmit Management Information - 選択されたインターフェイスについてLLDPフレームで管理アドレスを送信するかを指定する。

Optional TLV(s)

- **System Name - LLDPフレームにシステム名TLVを含む。**
- **System Description - LLDPフレームにシステム内容TLVを含む。**
- **System Capabilities - LLDPフレームにシステム機能TLVを含む。**
- **Port Description - LLDPフレームにポート内容TLVを含む。**

コマンドボタン

Apply/適用 ー 更新した画面をスイッチへ送ります。 変更はスイッチ上で有効化されますが保存しなければこれらの変更は電源を切ると保持されません。

8.2.11.3　**インターフェイス･サマリを見る**

Information

Interface Summary | Statistics | Local Info | Local Summary | Remote Info | Remote Summary

Interface	Link Status	Transmit	Receive	Notify	Optional TLV(s)	Transmit Management Information
Encl-CB1/0/1	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/2	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/3	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/4	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/5	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/6	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/7	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/8	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/9	Link Down	Enabled	Enabled	Enabled	System Name System Description	Yes

図：LLDP　インターフェイス･サマリ

構成不可能なデータ

Interface　-　LLDP - 802.1ABを構成できるすべてのポートを指定する。

Link Status - アップリンクかダウンリンクかのポートのリンク･ステータスを指定する。

Transmit - インターフェイスのLLDP - 802.1AB送信モードを指定する。

Receive - インターフェイスのLLDP - 802.1AB受信モードを指定する。

Notify - インターフェイスのLLDP - 802.1AB通知モードを指定する。

Optional TLV(s) - 含まれるLLDP - 802.1ABオプションTLVを指定する。

Transmit Management Information - LLDPフレームで管理アドレスを送信するかを指定する。

コマンドボタン

Refresh -　ページ情報を更新する。

8.2.11.4 **統計を見る**

Information

Interface Summary | Statistics | Local Info | Local Summary | Remote Info | Remote Summary

Last Update: 0 Days 00:00:00
Total Inserts: 0
Total Deletes: 0
Total Drops: 0
Total Ageouts: 0

Interface	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV Unknowns
Encl-CB1/0/1	0	0	0	0	0	0	0
Encl-CB1/0/2	0	0	0	0	0	0	0
Encl-CB1/0/3	0	0	0	0	0	0	0
Encl-CB1/0/4	0	0	0	0	0	0	0
Encl-CB1/0/5	0	0	0	0	0	0	0
Encl-CB1/0/6	0	0	0	0	0	0	0
Encl-CB1/0/7	0	0	0	0	0	0	0
Encl-CB1/0/8	0	0	0	0	0	0	0
Encl-CB1/0/9	0	0	0	0	0	0	0
Encl-CB1/0/10	0	0	0	0	0	0	0
Encl-CB1/0/11	0	0	0	0	0	0	0
Encl-CB1/0/12	0	0	0	0	0	0	0
Encl-CB1/0/13	0	0	0	0	0	0	0
Encl-CB1/0/14	0	0	0	0	0	0	0
Encl-CB1/0/15	0	0	0	0	0	0	0
Encl-CB1/0/16	0	0	0	0	0	0	0
Encl-CB1/0/17	0	0	0	0	0	0	0
Encl-CB1/0/18	0	0	0	0	0	0	0
Encl-CB1/0/19	0	0	0	0	0	0	0
Encl-CB1/0/20	0	0	0	0	0	0	0
Encl-CB1/0/21	0	0	0	0	0	0	0
Encl-CB1/0/22	0	0	0	0	0	0	0
Encl-CB1/0/23	0	0	0	0	0	0	0

図： LLDP 統計

構成不可能なデータ

Last Update - 遠隔システムと関連付けられたテーブルでエントリが生成、変更、削除された時間を指定する。

Total Inserts - 特定のMACサービス･アクセス･ポイント (MSAP)により報知された完全な情報セットが遠隔システムと関連付けられたテーブルに挿入された回数を指定する。

Total Deletes - 特定のMACサービス･アクセス･ポイント (MSAP)により報知された完全な情報セットが遠隔システムと関連付けられたテーブルから削除された回数を指定する。

Total Drops - 特定のMACサービス･アクセス･ポイント (MSAP)により報知された完全な情報セットが遠隔システムと関連付けられたテーブルに入力できなかった回数を指定する。

Total Age outs - 特定のMACサービス･アクセス･ポイント (MSAP)により報知された完全な情報セットが、情報タイミング間隔が有効期限を経過したため、遠隔システムと関連付けられたテーブルから削除された回数を指定する。

Interface - インターフェイスにスロット/ポートを指定する。

Transmit Total - LLDPエージェントが対応するポートで送信したLLDPフレーム数を指定する。

Receive Total - LLDPエージェントが有効化されている間に、対応するポートでLLDPエージェントが受信した有効なLLDPフレーム数を指定する。

Discards - LLDPエージェントが対応するポートでいかなる理由でも破棄したLLDP TLV数を指定する。

Errors - LLDPエージェントが有効化されている間に、対応するポートでLLDPエージェントが受信した無効なLLDPフレーム数を指定する。

Age outs - ポートで発生したエイジアウト回数を指定する。 合計エイジアウト数は、特定のMACサービス･アクセ

ス・ポイント (MSAP)により報知された完全な情報セットが、情報タイミング間隔が有効期限を経過したため、遠隔システムと関連付けられたテーブルから削除された回数を指す。

TLV Discards - LLDPエージェントが対応するポートでいかなる理由でも破棄したLLDP TLV数を指定する。

TLV Unknowns - LLDPエージェントが対応するポートで認識できなかった、ローカル・ポートで受信されたLLDP TLV数を指定する。

コマンドボタン

Refresh - ページ情報を更新する。

Clear - すべてのインターフェイスからLLDP統計を消去する。

8.2.11.5 ローカル情報を見る

Information

Interface Summary | Statistics | Local Info | Local Summary | Remote Info | Remote Summary

Interface: Encl-CB1/0/1
Chassis ID Subtype: MAC Address
Chassis ID: 00:23:8B:17:7B:85
Port ID Subtype: MAC Address
Port ID: 00:23:8B:17:7B:87
System Name:
System Description: FSC PRIMERGY BX900 GbE Connection Blade 36/12, L2+ Switch, Runtime
Port Description:
System Capabilities Supported: bridge
System Capabilities Enabled: bridge
Management Address: 00:23:8B:17:7B:85
Management Address Type: 802

Refresh

図：LLDPローカル情報

選択基準

Interface - LLDP - 802.1ABフレームを送信できるすべてのポートのリストを指定する。

構成不可能なデータ

Chassis ID Subtype - シャーシ識別子のソースを説明する文字列を指定する。

Chassis ID - ローカル・システムと関連付けられたシャーシ・コンポーネントを識別す るために使用される文字列値を指定する。

Port ID Subtype - ポート識別子のソースを説明する文字列を指定する。

Port ID - ポート識別子のソースを説明する文字列を指定する。

System Name - ローカル・システムのシステム名を指定する。

System Description - ローカル・システムと関連付けられた選択さ れたポートの内 容を指定する。

Port Description - ローカル・システムと関連付けられた選択さ れたポートの 内容を指定 する。

System Capabilities Supported - ローカル･システムのシステム機能を指定する。

System Capabilities Enabled - ローカル･システムのサポートされ有効化されたシステム機能を指定する。

Management Address- ローカル･システムの報知された管理アドレスを指定する。

Management Address Type - 管理アドレスのタイプを指定する。

コマンドボタン

Refresh - ページ情報を更新する。

8.2.11.6 ローカル･サマリを見る

Information

Interface Summary | Statistics | Local Info | Local Summary | Remote Info | Remote Summary

Interface	Port ID	Port Description
Encl-CB1/0/1	00:23:8B:17:7B:87	
Encl-CB1/0/2	00:23:8B:17:7B:87	
Encl-CB1/0/3	00:23:8B:17:7B:87	
Encl-CB1/0/4	00:23:8B:17:7B:87	
Encl-CB1/0/5	00:23:8B:17:7B:87	
Encl-CB1/0/6	00:23:8B:17:7B:87	
Encl-CB1/0/7	00:23:8B:17:7B:87	
Encl-CB1/0/8	00:23:8B:17:7B:87	
Encl-CB1/0/9	00:23:8B:17:7B:87	
Encl-CB1/0/10	00:23:8B:17:7B:87	
Encl-CB1/0/11	00:23:8B:17:7B:87	
Encl-CB1/0/12	00:23:8B:17:7B:87	
Encl-CB1/0/13	00:23:8B:17:7B:87	
Encl-CB1/0/14	00:23:8B:17:7B:87	
Encl-CB1/0/15	00:23:8B:17:7B:87	
Encl-CB1/0/16	00:23:8B:17:7B:87	
Encl-CB1/0/17	00:23:8B:17:7B:87	
Encl-CB1/0/18	00:23:8B:17:7B:87	
Encl-CB1/0/19	00:23:8B:17:7B:87	
Encl-CB1/0/20	00:23:8B:17:7B:87	
Encl-CB1/0/21	00:23:8B:17:7B:87	
Encl-CB1/0/22	00:23:8B:17:7B:87	
Encl-CB1/0/23	00:23:8B:17:7B:87	
Encl-CB1/0/24	00:23:8B:17:7B:87	
Encl-CB1/0/25	00:23:8B:17:7B:87	
Encl-CB1/0/26	00:23:8B:17:7B:87	
Encl-CB1/0/27	00:23:8B:17:7B:87	
Encl-CB1/0/28	00:23:8B:17:7B:87	
Encl-CB1/0/29	00:23:8B:17:7B:87	

図:LLDPローカルのサマリー

構成不可能なデータ

Interface - LLDP - 802.1ABフレームを送信できるポートを指定する。

Port ID - ポート識別子のソースを説明する文字列を指定する。

Port Description - ローカル･システムと関連付けられたポートの内容を指定する。

コマンドボタン

Refresh - ページ情報を更新する。

8.2.11.7　遠隔情報を見る

Information

Interface Summary | Statistics | Local Info | Local Summary | Remote Info | Remote Summary

Local Interface: Encl-CB1/0/48
Remote Device
Chassis ID Subtype: MAC Address
Chassis ID: 00:1E:68:85:F5:F1
Port ID Subtype: MAC Address
Port ID: 00:1E:68:85:F5:F3
System Name:
System Description: FSC PRIMERGY BX900 GbE Connection Blade 36/12, L2+ Switch, Runtime
Port Description:
System Capabilities Supported: bridge
System Capabilities Enabled: bridge
Time to Live: 113
Management Address:

Address	Type
192.168.2.1	IPv4

Refresh

図： LLDP 遠隔情報

選択基準

Local Interface - LLDPフレームを受信できるすべてのローカル･ポートをを指定する。

構成不可能なデータ

Chassis ID Subtype - シャーシ識別子のソースを指定する。

Chassis ID - リモート･システムと関連付けられたシャーシ･コンポーネントを指定する。

Port ID Subtype - ポート識別子のソースを指定する。

Port ID - リモート･システムと関連付けられたポート･コンポーネントを指定する。

6**System Name** - リモート･システムのシステム名を指定する。

System Description - リモート･システムと関連付けられた所与のポートの内容を指定する。

Port Description - リモート･システムと関連付けられた所与のポートの内容を指定する。

System Capabilities Supported - リモート･システムのシステム機能を指定する。

System Capabilities Enabled - リモート･システムのサポートされ有効化されたシステム機能を指定する。

Time to Live/TTL - 受信されたリモート･エントリのTTL値を秒数で指定する。

管理アドレス

- **Management Address** - リモート･システムの通知された管理アドレスを指定する。
- **Type** - 管理アドレスのタイプを指定する。

コマンドボタン

Refresh - ページ情報を更新する。

8.2.11.8 リモート･サマリを見る

Information

Interface Summary | Statistics | Local Info | Local Summary | Remote Info | Remote Summary

Local Interface	Chassis ID	Port ID	System Name
Encl-CB1/0/48	00:1E:68:85:F5:F1	00:1E:68:85:F5:F3	

Refresh　Clear

図：LLDP リモート･サマリ

構成不可能なデータ

Local Interface リモート･システムにより報知されたLLDPフレームを受信できるローカル･ポートを指定する。

/シャーシID - リモート･システムと関連付けられたシャーシ･コンポーネントを指定する。.

Port ID - リモート･システムと関連付けられたポート･コンポーネントを指定する。.

System Name - リモート･システムのシステム名を指定する。

コマンドボタン

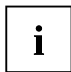
Refresh - ページ情報を更新する。

Clear - すべてのインターフェイスで受信されたLLDPリモートデバイス情報を消去する。

8.2.12 DHCPクライアント

8.2.12.1 DHCPクライアント識別子

スイッチ用のDCHPクライアント識別子を特定する DHCPクライアント識別子はDHCPサーバとのすべての通信にクライアント識別子を含むために使用される。 識別子タイプはDHCPサーバの要件によって異なる。



DHCPクライアント識別子はホスト名が変更されると構成で直ちに変更される。 新たなDHCPクライアント識別子を作動させるためには更新操作(再起動または"oob protocol none“ または “oob protocol dhcp"(OOBプロトコル無しとOOBプロトコルHDCP"コマンド)が必要である。

DHCP Client
DHCP Client-Identifier | DHCP Restart | DHCP6 Restart
Current DHCP Identifier Text: CB.SQ834LW00001
DHCP Identifier: Default
Apply

図 ： DHCP クライアント識別子

選択基準

DHCP Identifier - DHCP識別子の種類を指定する。

- デフォルト
- 特定の文字列
- 特定の 16 進数値

構成不可能なデータ

Current DHCP Identifier (Hex/Text) - DHCP識別子の現在の設定を表示する。

構成可能データ

Text String - 文の文字列。

Hex Value - 16 進数値。

コマンドボタン

Apply - 更新した画面をスイッチへ送り、DHCPクライアント識別子の設定を実施する

8.2.12.2 DHCP再起動

このコマンドはBOOTPまたはDHCPクライアント要求を、ip addressコマンドによりBOOTPまたはDHCPモードに設定された任意のIPインターフェイスに発行する。 DHCPはサーバがクライアントの最後のアドレスがあるならそれを再割当てするよう要求する。 BOOTPまたはDHCPサーバが別のドメインに移動された場合、クライアントに発行されたアドレスのネットワーク部分は新たなドメインに基づくことになる。

DHCP Client		
DHCP Client-Identifier	DHCP Restart	DHCP6 Restart

Use the function to initiate a BOOTP or DHCP client requent

Reset

図： DHCP 再起動

コマンドボタン

Reset - 更新した画面をスイッチへ送りDHCPクライアントの再スタートを実施する

8.2.12.3 DHCP6 再起動

このコマンドはDHCP6 クライアント要求を、ip addressコマンドによりDHCPモードに設定された任意のIPインターフェイスに発行する。 DHCPはサーバがクライアントの最後のアドレスがあるならそれを再割当てするよう要求する。 DHCPサーバが別のドメインに移動された場合、クライアントに発行されたアドレスのネットワーク部分は新たなドメインに基づくことになる。

DHCP Client		
DHCP Client-Identifier	DHCP Restart	DHCP6 Restart

Use the function to restart DHCP6 client.

Reset

図：DHCP6 再起動

コマンドボタン

Reset - 更新した画面をスイッチへ送りDHCP6 クライアントの再スタートを実施する

8.2.13 DNSリレー

8.2.13.1 DNSリレー・コンフィグ

DNSプロトコルはドメイン名システム(DNS)、すなわちホスト名をIPアドレスへマッピングするための分散型のデータベース、を制御します。スイッチのDNSを構成するときIPアドレス用のホスト名をすべてIPコマンド、たとえばピング、Telnet 、Traceroute、および関連したTelnet のサポート操作等、で代用できます。 ドメイン名を追跡するためIPではドメイン・ネーム・サーバというコンセプトが定義されており、これにはIPアドレスに対応させた名前のキャッシュ (すなわちデータベース) がある。 ドメイン名とIPアドレスを対応させるには、まずホスト名を定義し、ネットワークにあるネームサーバを指定してからDNSを有効化しなければならない。

DNS Relay

DNS Relay Config | Domain Name Config | Name Server Config | DNS Cache Summary | Hosts Config

Admin Mode: Disable

Default Domain Name:

Apply

図 : DNS リレー・コンフィグ

選択基準

Admin Mode - プルダウン・メニューから有効化または無効化を選択する。 'enable' (有効化)を選択すると、IPドメイン・ネーミング・システム (DNS)によるホスト名とアドレスの変換が有効化される。

構成可能データ

Default Domain Name - 未認定のホスト名を完了させるために使用されるデフォルト・ドメイン名 未認定の名前をドメイン名から分離する初期フェーズは含めないこと。 これは 63 文字までの文字列である。

コマンドボタン

Apply - 更新した構成をスイッチへ送ります。構成の変更は即時に有効化されます。 これらの変更は、保存しなければ電源を切ると保持されません。

8.2.13.2 ドメイン名コンフィグ

不完全なホスト名（すなわち、ピリオド表記でフォーマットされていないクライアントから渡されたホスト名）に付加できるドメイン名の構成パラメータを変更するためにこの画面は使用できる。 テーブルの内容を表示するためにもこの画面を使用できる。

DNS Relay
DNS Relay Config | Domain Name Config | Name Server Config | DNS Cache Summary | Hosts Config
Domain: Create
Domain Name:*
* = mandatory
Apply Delete All

図： DNS リレー・ドメイン名コンフィグ

選択基準

Domain - 追加の"Create".オプション付きで既存のドメイン名をすべて指定する。 "Create"を選択すると別のテキストボックス"Domain Name"が表示され、ここには構成するドメイン名を入力できる。

構成可能データ

Domain Name - ドメイン名を指定する。 未設定の名前をドメイン名から分離するピリオドは含めないこと。 これは63 文字までの文字列である。

コマンドボタン

Apply - 更新した構成をスイッチへ送る。構成の変更は即時に有効化されます。

Delete - ドメイン名の入力を削除する。更新した構成をスイッチへ送る。構成の変更は即時に有効化されます。.

Delete All - すべてのドメイン名の入力を削除する。 更新した構成をスイッチへ送る。構成の変更は即時に有効化されます。

8.2.13.3　ネームサーバ･コンフィグ

ドメイン･ネームサーバの構成パラメータを変更するためにこの画面を使用できる。 テーブルの内容を表示するためにもこの画面を使用できる。

DNS Relay
DNS Relay Config | Domain Name Config | Name Server Config | DNS Cache Summary | Hosts Config
Name Server: Create
IP Address:* 0 . 0 . 0 . 0
* = mandatory
Apply

図： DNS リレー･ネームサーバ･コンフィグ

選択基準

Name Server - 追加の"Create".オプション付きで既存のドメイン･ネームサーバをすべて指定する。 "Create"を選択すると別のテキストボックス"IP Address"が表示され、ここには構成するドメイン･ネームサーバを入力できる。

構成可能データ

IP Address - ドメイン･ネームサーバのアドレスを指定する

構成不可能なデータ

Request - 直前のエージェント再起動以降のDNS要求数を指定する。

Response - 直前のエージェント再起動以降のDNSサーバ応答数を指定する。

コマンドボタン

Apply - 更新した構成をスイッチへ送る。構成の変更は即時に有効化されます。

Delete - ドメイン･ネームサーバエントリを削除する。 更新した構成をスイッチへ送る。構成の変更は即時に有効化されます。

Delete All - すべてのドメイン･ネームサーバ･エントリを削除する。更新した構成をスイッチへ送る。 構成の変更は即時に有効化されます。

Clear All Counter - すべてのネームサーバ･カウンターをクリアする。

8.2.13.4 DNSキャッシュ･サマリ

ﾄﾞﾒｲﾝ･ﾈｰﾑ･ｼｽﾃﾑ (DNS)はIPｱﾄﾞﾚｽにﾄﾞﾒｲﾝ名を動的にマップする。 このパネルはDNSキャッシュの現在の内容を表示する。

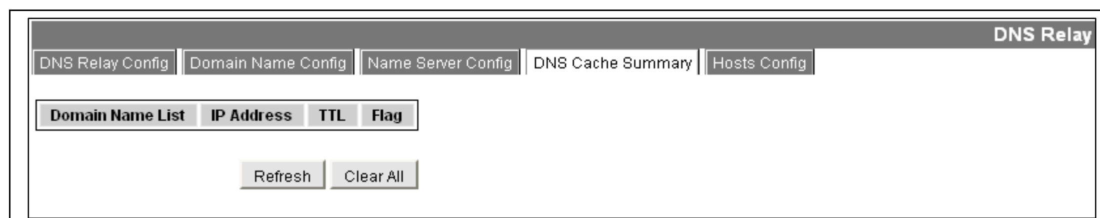


図 : DNS キャッシュ･サマリ

構成不可能なデータ

Domain Name List - このレコードに関連付けられたﾄﾞﾒｲﾝ･ﾈｰﾑ

IP address - このレコードに関連付けられたIPｱﾄﾞﾚｽ。

TTL - ネームサーバによりリポートされたTimeToLive。

Flag - レコードのフラグ。

コマンド･ボタン

Refresh - 最新のDNSキャッシュ･エントリにより頁を更新する。

Clear All - DNSキャッシュ内すべてのエントリを消去する。

8.2.13.5 **ホスト･コンフィグ**

DNSテーブルにある静的エントリの構成パラメータを変更するためにこの画面を使用できる。 テーブルの内容を表示するためにもこの画面を使用できる。

DNS Relay

DNS Relay Config | Domain Name Config | Name Server Config | DNS Cache Summary | Hosts Config

Domain: Create

Domain Name:*

IP Address:* 0 . 0 . 0 . 0

* = mandatory

Apply　Delete All

図 ：DNS リレー･ホスト･コンフィグ

選択基準

Domain - 追加の"Create".オプション付きで既存のホストをすべて指定する。 "Create"を選択すると別のテキストボックス"Domain Name"が表示され、ここには構成するホストを入力できる。

構成可能データ

Domain Name - ホストのドメイン名を指定する。 これは 63 文字までの文字列である。

IP Address - ホストのIPアドレスを指定する。

コマンドボタン

Apply - 更新した構成をスイッチへ送る。構成の変更は即時に有効化されます。

Delete - ホストの入力を削除する。更新した構成をスイッチへ送る。構成の変更は即時に有効化されます。

Delete All - すべてのホストの入力を削除する。更新した構成をスイッチへ送る。構成の変更は即時に有効化されます。

8.2.14 IPv6

8.2.14.1 統計

IPv6

Statistics

Management Type: In-Band

IPv6 Statistics	
Total Datagrams Received	0
Received Datagrams Locally Delivered	0
Received Datagrams Discarded Due To Header Errors	0
Received Datagrams Discarded Due To MTU	0
Received Datagrams Discarded Due To No Route	0
Received Datagrams With Unknown Protocol	0
Received Datagrams Discarded Due To Invalid Address	0
Received Datagrams Discarded Dut To Truncated Data	0
Received Datagrams Discarded Other	0
Received Datagrams Reassembly Required	0
Datagrams Successfully Reassembled	0
Datagrams Failed To Reassemble	0
Datagrams Forwarded	0
Datagrams Locally Trasmitted	2
Datagrams Transmit Failed	0
Datagrams Successfully Fragmented	0
Datagrams Failed To Fragment	0
Datagrams Fragments Created	0
Multicast Datagrams Received	0
Multicast Datagrams Transmitted	2
ICMPv6 Statistics	
Total ICMPv6 Messages Received	0
ICMPv6 Messages With Errors Received	0
ICMPv6 Destination Unreachable Messages Received	0
ICMPv6 Messages Prohibited Administratively Received	0

図： IPv6 統計

選択基準

Management Type - 構成すべきポート･タイプを指定する。この選択が変更されると、画 面が更新されてす べての欄は新たに選択されたポート･タイプに更新される。

構成不可能なデータ

IPv6 統計

Total Datagrams Received - インターフェイスにより受信された入力データグラムの総数、エラー有りで受信されたものを含む。

Received Datagrams Locally Delivered - IPv6 ユーザー･プロトコル (ICMPを含む) に送信が完了したデータグラム合計数。 このカウンターはデータグラムの一部のための入力インターフェイスではないことがある当該データグラムが宛てられたインターフェイスで 1 ずつ増加される。

Received Datagrams Discarded Due To Header Errors- バージョン不一致、他のフォーマット･エラー、ホップ数の超過、IPv6の処理中に発見されたエラー等を含むIPv6ヘッダーにあるエラーが原因で破棄された入力データグラム数。

Received Datagrams Discarded Due To MTU - 入力データグラムのうちそのサイズがアウトバウンド･インターフェイスのリンクMTUを超過したために転送できなかった入力データグラム数。

Received Datagrams Discarded Due To No Route - ターゲットに送信するためのルートが見つからなかったために破棄された入力データグラム数。

Received Datagrams With Unknown Protocol - 受信には成功したがプロトコルが不明またはサポートされないため破棄されたローカルに宛てられたデータグラム数。 このカウンターはデータグラムの一部のための入力インターフェイスではないことがある当該データグラムが宛てられたインターフェイスで 1 ずつ増加される。

Received Datagrams Discarded Due To Invalid Address - IPv6 ヘッダーのターゲット欄にあるIPv6 アドレスがこのエンティティで受信されるために有効なアドレスではなかったために破棄された入力データグラム数。 この計数には無効アドレス (たとえば、::9)やサポートされないアドレス(たとえば、未割当てのプレフィックス付きアドレス) を含む。 IPv6 ルーターではないためデータグラムを転送しないエンティティについては、このカウンターはターゲット・アドレスがローカル・アドレスでなかったために破棄されたデータグラムを含む。

Received Datagrams Discarded Dut To Truncated Data - データグラム・フレームに十分なデータがないために破棄された入力データグラム数。

Received Datagrams Discarded Other - 処理継続を中断すべき問題がないにもかかわらず破棄された(たとえば、バッファー・スペースの欠如等) 入力IPv6 データグラム数。 このカウンターが再アセンブリを待機中に破棄されたデータグラムを含まないことに注意する。

Received Datagrams Reassembly Required - このインターフェイスで再アセンブリを要する受信IPv6フラグメント数。 このカウンターはフラグメントの一部のための入力インターフェイスではないことがある当該フラグメントが宛てられたインターフェイスで 1 ずつ増加される。

Datagrams Successfully Reassembled - IPv6 再アセンブリが成功したデータグラム数。 このカウンターはフラグメントの一部のための入力インターフェイスではないことがある当該データグラムが宛てられたインターフェイスで 1 ずつ増加される。

Datagrams Failed To Reassemble - (タイムアウトやエラー等なんらかの理由で) IPv6再アセンブリ・アルゴリズムにより検出 された障害数。 一部のアルゴリズム(特にRFC815 のアルゴリズム)はフラグメントを受信されると結合させることによりフラグメント数を追跡できなくなるため、この値は破棄されたIPv6フラグメントでは必ずしもないことに注意する。 このカウンターはフラグメントの一部のための入力インターフェイスではないことがある当該フラグメントが宛てられたインターフェイスで 1 ずつ増加される。

Datagrams Forwarded - このエンティティが受信し最終ターゲットに転送した出力データグラム数。 IPv6ルーターとしては機能しないエンティティの場合、このカウンターhこのエンティティを通してソース・ルートされ、ソース・ルート処理に成功したパケットのみを含む。 転送が成功したデータグラムについてアウトバウンド・インターフェイスのカウンターはインクリメントされる。

Datagrams Locally Transmitted - この出力インターフェイスからこのエンティティが送信に成功したデータグラム数。

Datagrams Transmit Failed - このエンティティが送信に失敗したデータグラム数。

Datagrams Successfully Fragmented - この出力インターフェイスでフラグメント化に成功したIPv6 データグラム数。

Datagrams Failed To Fragment - この出力インターフェイスでフラグメント化に失敗したIPv6 データグラム数。

Datagrams Fragments Created - この出力インターフェイスでフラグメント化の結果生成された出力データグラム・フラグメント数

Multicast Datagrams Received - インターフェイスに受信されたマルチキャスト・パケット数。

Multicast Datagrams Transmitted - インターフェイスにより送信されたマルチキャスト・パケット数。

ICMPv6 統計

Total ICMPv6 Messages Received - ipv6IfIcmpInErrorsコマンドにより計数されたものをすべて含むICMPメッセージの合計数。 このインターフェイスはメッセージのための入力インターフェイスではないことがある当該ICMPメッセージが宛てられたインターフェイスであることに注意する。

ICMPv6 Messages With Errors Received - インターフェイスが受信したがICMP固有エラー(間違ったICMPチェックサム、間違った長さ等)があると判断された ICMPメッセージ数。

ICMPv6 Destination Unreachable Messages Received - インターフェイスが受信したICMPv6ターゲット未到達

メッセージ数。

ICMPv6 Messages Prohibited Administratively Received - インターフェイスが受信したICMPｖ6ターゲット未到達で通信管理上禁止されたメッセージ数。

ICMPv6 Time Exceeded Messages Received - インターフェイスが受信したICMPｖ6時間超過メッセージ数。

ICMPv6 Parameter Problem Messages Received - インターフェイスが受信したICMPｖ6パラメータ障害有りのメッセージ数。

ICMPv6 Packet Too Big Messages Received - インターフェイスが受信したICMPｖ6過大パケットサイズメッセージ数。

ICMPv6 Echo Request Messages Received - インターフェイスが受信したICMPｖ6エコー要求メッセージ数。

ICMPv6 Echo Reply Messages Received - インターフェイスが受信したICMPｖ6エコー応答メッセージ数。

ICMPv6 Router Solicit Messages Received - インターフェイスが受信したICMPｖ6ルーター要請メッセージ数。

ICMPv6 Router Advertisement Messages Received - インターフェイスが受信したICMPｖ6ルーター通知メッセージ数。

ICMPv6 Neighbor Solicit Messages Received - インターフェイスが受信したICMPｖ6ネイバー要請メッセージ数。

ICMPv6 Neighbor Advertisement Messages Received - インターフェイスが受信したICMPｖ6ネイバー通知メッセージ数。

ICMPv6 Redirect Messages Received - インターフェイスが受信したICMPｖ6リダイレクト･メッセージ数。

ICMPv6 Group Membership Query Messages Received - インターフェイスが受信したICMPｖ6グループ･メンバーシップ･クエリー･メッセージ数。

ICMPv6 Group Membership Response Messages Received - インターフェイスが受信したICMPｖ6グループ･メンバーシップ応答メッセージ数。

ICMPv6 Group Membership Reduction Messages Received - インターフェイスが受信したICMPｖ6グループ･メンバーシップ削メッセージ数。

Total ICMPv6 Messages Transmitted - このインターフェイスが送信を試行したICMPメッセージ総数。 このカウンターはすべてのicmpOutErrorsコマンドが計数したものを含むことに注意する。

ICMPv6 Messages Not Transmitted Due To Error - バッファー欠如等のICMP内で発見された障害によりこのインターフェイスが送信しなかったICMPメッセージ数。 この値にはIPｖ6が結果データグラムをルートできないこと等のICMPレイヤー外で発見されたエラーは含まない。 実装によってはこのカウンターの値に影響しないタイプのエラーがあることがある。

ICMPv6 Destination Unreachable Messages Transmitted - インターフェイスが送信したICMPｖ6ターゲット到達不可メッセージ数。

ICMPv6 Messages Prohibited Administratively Transmitted - 送信されたがICMPターゲット到達不可や通信管理上禁止されたメッセージ数。

ICMPv6 Time Exceeded Messages Transmitted - インターフェイスが送信したICMPｖ6時間超過メッセージ数。

ICMPv6 Parameter Problem Messages Received - インターフェイスが送信したICMPｖ6パラメータ障害有りのメッセージ数。

ICMPv6 Packet Too Big Messages Transmitted - インターフェイスが送信したICMPｖ6過大パケットサイズメッセージ数。

ICMPv6 Echo Request Messages Transmitted - インターフェイスが送信したICMPｖ6エコー(要求)メッセージ数。

ICMPv6 Echo Reply Messages Transmitted- インターフェイスが送信したICMPエコー応答メッセージ数。

ICMPv6 Router Solicit Messages Transmitted - インターフェイスが送信したICMPネイバー要請メッセージ数。

ICMPv6 Router Advertisement Messages Transmitted - インターフェイスが送信したICMPルーター通知メッセ

ージ数。

ICMPv6 Neighbor Solicit Messages Transmitted - インターフェイスが送信したICMPネイバー要請メッセージ数。

ICMPv6 Neighbor Advertisement Messages Transmitted - インターフェイスが送信したICMPネイバー通知メッセージ数。

ICMPv6 Redirect Messages Transmitted - 送信されたICMPv6 リダイレクト・メッセージ数。

ICMPv6 Group Membership Query Messages Transmitted - 送信されたICMPv6グループ・メンバーシップ・クエリー・メッセージ数。

ICMPv6 Group Membership Response Messages Transmitted - 送信されたICMPv6グループ・メンバーシップ応答メッセージ数。

ICMPv6 Group Membership Reduction Messages Transmitted - 送信されたICMPv6グループ・メンバーシップ削除メッセージ数。

ICMPv6 Duplicate Address Detects - インターフェイスが検出した重複アドレス数

コマンドボタン

Clear - IPv6 統計を消去する。

Refresh -　最新データで更新します。

8.3　スイッチングのメニュー

この節はスイッチポート、ポートベースのVLAN、プロトコルベースのVLAN、 GARP、IGMPスヌーピング、ポートチャンネル、スパニングツリー、及び、802.1pプライオリティマッピングとポートのセキュリティ等をユーザーが構成できるようにします。

8.3.1　転送データベース

8.3.1.1　構成

このパネルにより転送データベースのためのアドレスのエイジング･タイムアウトを設定します。

Forwarding Database

Config | Search

Aging Interval (secs) (10 to 1000000):* 300

* = mandatory

Apply

図 ： 転送データベースの構成

構成可能データ

Aging Interval (secs)　- 転送デーベースには、決して古くならない静的なエントリと、特定の時間内に更新されなければ削除されてしまう動的に習得したエントリが含まれます。数値を入力してアドレスのエイジング間隔タイムアウト時間を指定してください。10 から 1000000 までの任意の秒数を入力できます。

IEEE 802.1Dは工場出荷時デフォルト値 300 秒を初期値として推奨しています。

コマンドボタン

Apply - 画面の設定をスイッチに更新します。。 パワーサイクル後、設定を保持するには保存してください。。

8.3.1.2 検索

このパネルにより転送データベースのエントリの情報を表示します。これらのエントリは受信したフレームを転送する方法を決定するための透過的ブリッジ機能によって使用されます。

Forwarding Database

Config | Search

Filter: All

MAC Address Search: [ ] Search

MAC Address	Source Slot/Port(s)	ifIndex	Status
00:01:00:23:8B:17:7B:85	Encl-CB1/3/1	49	Management

Refresh

図 : 転送データベースの検索

選択基準

Management Unit – 転送データベーステーブルが表示される管理ユニットを表示する。

Filter – 表示するエントリを指定する。

- **Learned**:「learned」を選択すると習得されたMACアドレスのみ表示されます**All:「すべて」を選択すればテーブル全体が表示されます。**

構成可能データ

MAC Address Search – 個々のMACアドレスを検索することもできます。コロンで区切られた 2 桁のグループの形式で、2 バイトの 16 進法でVLAN IDを入力しそれに続 けて 6 バイトの 16 進表記のMACアドレスを入力します。たとえば 01:23:45:67:89:AB:CD:EF なら、01:23 がVLAN IDで、45:67:89:AB:CD:EFがMACアドレスです。次に検索ボタンをクリックします。アドレスが存在すれば最初のエントリにはそのエントリが表示され、残りの(大きな方の)MACアドレスがそれに続く。正確な一致が要求されます。

構成不可能なデータ

MAC Address – スイッチが転送またはフィルタリングの情報を持っているユニキャストのMACアドレス。形式は 2 バイトの 16 進法VLAN ID番号とそれに続く 6 バイトのMACアドレスです。たとえば 01:23:45:67:89:AB:CD:EF なら、01:23 がVLAN IDで 45:67:89:AB:CD:EFがMACアドレスです。

Source Port – このアドレスが学習されたポート。-すなわち、MACアドレスが到達できるポート。

ifIndex – ソースポートに関連したMIBインターフェイステーブル・エントリのインターフェイス番号です。

Status– このエントリのステータス。可能な数値は;

- **Static**: 静的なMACフィルターが定義されたとき追加されたエントリ。
- **Learned**: 受信トラフィックの送信元MACアドレスを監視して学習され、現在使われているエントリ。
- **Management**: インターフェイス 0.1 により識別されるシステムMACアドレス
- **Self**: スイッチの物理インターフェイスの中の 1 個のMACアドレス

コマンドボタン

Search– 特定のMACアドレスを検索する

Refresh - データベースを再取得し、テーブルの最初のエントリから改めて表示します。

8.3.2 ポート

8.3.2.1 構成

Port

Config | Summary | Mirroring

Slot/Port: All
Port Type:
STP Mode: Enable
Admin Mode: Enable
E-Keying Status:
LACP Mode: Enable
Physical Mode: Auto
Physical Status:
Link Status:
Link Trap: Enable
Maximum Frame Size (1518 to 9216) :* 1518
ifIndex:
Flow Control: Disable
Broadcast Storm Control: Disable
Multicast Storm Control: Disable
Unicast Storm Control: Disable
Capability: 10 Mbps Half Duplex / 10 Mbps Full Duplex / 100 Mbps Half Duplex / 100 Mbps Full Duplex / 1000 Mbps Full Duplex

* = mandatory

Apply

図 : ポートの構成

選択基準

Slot/Port - データが表示されるまたは構成されるインターフェイスを選択する

STP Mode– ポートやLAGのためにスパニングツリー･プロトコルの管理モードを選択します。可能な値は;

- 有効 – これを選ぶと、このポートへのスパニングツリープロトコルが有効化されます
- 無効 – これを選ぶと、このポートへのスパニングツリープロトコルが無効化されます。

Admin Mode - プルダウン･メニューでポート制御管理ステートを選択する。 ポートをネットワークに参加させるには'enable'(有効化する)を選択する。 デフォルト設定は有効化されている。

LACP Mode – リンク･アグリゲーション制御プロトコルの管理状態を選択します。モードはポートがリンクアグリゲーションに参加できるように有効化されなければなりません。プルダウン入力欄で対応する行を選び有効化または無効化できます。工場出荷時デフォルトは有効です。

Physical Mode- プルダウン･メニューでポートの速度と二重モードを選択する。 autoを選択すると、二重モードと速度が自動ネゴシエーションにより設定される。 ポートの最高性能 (全二重で 100Mbps)が通知されることに注意する。 その他のポートの二重モードと転送速度は選択できる。 工場側デフォルトはautoである。 スロット/ポートで"All"オプションに適用された選択がすべての該当インターフェイスのみに適用される。

Link Trap- このオブジェクトはリンク･ステータスが変化したときトラップを送るかを定義する。 デフォルト設定は有効化されている。

Flow Control/Flow Control - 選択されたインターフェイスでフロー制御を有効化または無効化するために使用される。

Broadcast Storm Control – 選択したインターフェイスのブロードキャスト･ストームの機能を有効化または無効化するために使う。ブロードキャスト･ストーム制御の値はレベル 1、レベル 2、レベル 3、とレベル 4 が可能です。

- ブロードキャスト･ストーム、マルチキャスト･ストーム、 及び、 ユニキャスト･ストームが下に説明されます。
- スイッチ用の実際のパケット速度はそのインターフェイス(表 1 と表 2 を参照)の入力レベルと速度から変換されます。

10/100Mbps/1Gbpsのテーブル

レベル	パケット速度(pps)
1	64
2	128
3	256
4	512

10Gbpsのテーブル

レベル	パケット速度(pps)
1	1042
2	2084
3	3124
4	4167

Multicast Storm Control- 選択されたインターフェイスのマルチキャスト･ストーム機能を有効化または無効化するために使われる。マルチキャストストーム制御の値はレベル 1、レベル 2、 レベル 3、 レベル 4 から選ぶ。

Unicast Storm Control- 選択されたインターフェイスのユニキャスト･ストーム機能を有効化または無効化するために使われる。ユニキャストストーム制御の値はレベル 1、レベル 2、 レベル 3、 レベル 4 から選ぶ。

構成可能データ

Maximum Frame Size- イーサネット･ヘッダー、CRC、ペイロードを含みインターフェイスがサポートするまたは構成された最大イーサネット･フレーム･サイズ (1518 から 9216). デフォルト最大フレーム･サイズは 1518 である。

Capability - 自動ネゴシエーション中に所与のインターフェイスのポート機能を通知できる。

Port Description - ポートに付属する内容説明文字列。 最大 64 文字まで可能である。

構成不可能なデータ

Port Type - 普通のポートではこの欄は空白となる。 可能な値:

- Source/ソース - ポートは監視ポートである。 詳細はポート監視画面に出ている。
- Destination/ターゲット - ポートは監視ポートである。 詳細はポート監視画面に出ている。
- Port Channel/ポート･チャネル - ポートはリンクアグリゲーション･ トランクのメンバーである。 詳細はLAG画面に出ている。

E-Keying Status - E-KEY･ステータスを示す。

Physical Status- ポート速度と二重モードを示す。

Link Status- リンクがアップかダウンかを示す。

ifIndex - このポートと関連付けられたインターフェイス･テーブルの番号。

コマンド･ボタン

Apply - 入力した数値でスイッチを更新する。 もし、設定が保存されていない場合は、パワーサイクル後、設定はほじされません.

8.3.2.2 サマリ

この画面はスイッチのすべてのポートのステータスを表示する。

Port

Config | Summary | Mirroring

MST ID: CST

Slot/Port	Port Type	STP Mode	Forwarding State	Port Role	Admin Mode	E-Keying Status
Encl-CB1/0/1		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/2		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/3		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/4		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/5		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/6		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/7		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/8		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/9		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/10		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/11		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/12		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/13		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/14		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/15		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/16		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/17		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/18		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/19		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/20		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/21		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/22		Enabled	Disabled	Disabled	Enable	Connecte
Encl-CB1/0/23		Enabled	Disabled	Disabled	Enable	Connecte

図　ポートのサマリー

選択基準

MST ID – 現在構成されているMST IDのリストからマルチプル・スパニングツリーのインスタンスを選びスパニングツリーのパラメータを表示するための値を決定する。選択されたMST IDを変更すると画面の更新が作成される。スパニングテストが無効化されている場合、これはセレクターではなくCSTという静的な値になります。

構成不可のポート・ステータス・データ

Slot/Port - ポートを識別する。

Port Type- 普通のポートではこの欄は空白となる。 可能な値:

- Source/ソース - ポートは監視ポートである。 詳細はポート監視画面に出ている。
- Destination/ターゲット - ポートは監視ポートである。 詳細はポート監視画面に出ている。
- Port Channel/ポート・チャネル - ポートはリンクアグリゲーション・ トランクのメンバーである。 詳細はLAG画面に出ている。

STP Mode: ポートまたはLAGに関連したスパニングツリープロトコル管理モード。可能な値は:

- 有効- スパニングツリーがこのポートで有効になる
- スパニングツリーがこのポートで無効になる

Forwarding State- ポートの現在のステートがスパニング・ツリー・ ステートである。 このステートはフレーム受信時にポートが行う動作を制御する。 ブリッジがポート障害を検出すると、そのポートを故障状態に変更する。 他の5 個のステートは次のIEEE 802.1Dに定義される項目である：無効

- ブロッキング
- リスニング
- ラーニング

- 転送

Port Role – 有効化された各MSTブリッジポートには各スパニングツリーのためにポ ートロールが割当てられる。このポートロールは以下の値のひとつです。ルートポート、代表ポート、バックアップ･ポート、マスター･ポート、または無効のポート。

Admin Mode - ポート制御管理ステート。 ポートはネットワークに許可される には有効化されていなければならない。 デフォルト設定は有効化されている。

E-KEY･ステータス - ポートのE-KEY･ステータスを示す。

LACP Mode – リンク･アグリゲーション制御プロトコルの管理状態を表示します。このモードはポートがリンク･アグリゲーションに参加できるように有効化されていなければなりません。

Physical Status - ポート速度と二重モードを示す。 自動ネゴシエーション･モードでは二重モードと速度は自動ネゴシエーションで設定される。

Physical Status - ポート速度と二重モードを示す。

Link Status - リンクがアップかダウンかを示す。

Link Trap- リンク状態の変化時にポートがトラップを送るかを示す。

ifIndex - このポートと関連付けられたインターフェイス･ テーブルの番号。

Flow Control - このポートでのフロー制御の状態を示す。

Broadcast Storm Controlームの制御 – ブロードキャストストーム制御 のステータスを表示する。無効、レベル 1、レベル 2、レベル 3、レベル 4

Multicast Storm Control – マルチキャストストーム制御 のステータスを表示する。無効、レベル 1、レベル 2、レベル 3、レベル 4

Unicast Storm Control – ユニキャストストーム制御のステ ータスを表示する。無効、レベル 1、レベル 2、レベル 3、レベル 4

Capability - 自動ネゴシエーション中のポート機能を示す。

Port Description - ポートの内容を示す。

コマンドボタン

Refresh - 画面を最新データで更新する。

8.3.2.3 ミラーリング

Port
Config | Summary | Mirroring
Session: 1
Mode: Disable
Source Port(s):
Destination Port:
Add Source Port | Apply | Delete

図 : ポート･ミラーリング

選択基準

Session ID- リストからポート･ミラーリング･セッションを選択する。 許可されるセッション数はプラットフォームに依存する。 デフォルトでは最初のセッ ションが選択されている。 最大 1 個のセッションがサポートされる。

Mode- 選択されたセッションIDのセッション･モードを指定する。 デフォルトのセッション･モードは無効化である。

Destination Port - プローブ･ポートとして機能し、構成されたミラー化ポ ートからすべてのトラフィックを取得する。デフォルト値は空白である。

構成可能データ

Source Port(s) - 方向及びモニター先･ポートをミラー･ポートに指定する。 送信元･ポートのトラフィックがプローブ･ポートに送られる。 最大 48 ソース･ポートをセッション毎に選択できる。

コマンド･ボタン

Add Source Ports- 選択されたセッションに送信元･ポートを追加する。

Remove Source Ports - 選択されたセッションの構成された送信元･ポ ートを削除する.

Apply - 更新した画面をスイッチへ送り､変更がスイッチで有効化されるようにする。

Delete - 選択されたセッション構成を削除する。

8.3.3 VLAN

8.3.3.1 構成

VLAN

Config | Status | Port Config | Port Summary | Reset Config

VLAN ID and Name: 1 - Default
VLAN ID : 1
VLAN Name: Default
VLAN Type: Default
Page: 1

Slot/Port	Status	Participation	Tagging
All			
Encl-CB1/0/1	Include	Include	Untagged
Encl-CB1/0/2	Include	Include	Untagged
Encl-CB1/0/3	Include	Include	Untagged
Encl-CB1/0/4	Include	Include	Untagged
Encl-CB1/0/5	Include	Include	Untagged
Encl-CB1/0/6	Include	Include	Untagged
Encl-CB1/0/7	Include	Include	Untagged
Encl-CB1/0/8	Include	Include	Untagged
Encl-CB1/0/9	Include	Include	Untagged
Encl-CB1/0/10	Include	Include	Untagged
Encl-CB1/0/11	Include	Include	Untagged
Encl-CB1/0/12	Include	Include	Untagged
Encl-CB1/0/13	Include	Include	Untagged
Encl-CB1/0/14	Include	Include	Untagged
Encl-CB1/0/15	Include	Include	Untagged
Encl-CB1/0/16	Include	Include	Untagged
Encl-CB1/0/17	Include	Include	Untagged
Encl-CB1/0/18	Include	Include	Untagged
Encl-CB1/0/19	Include	Include	Untagged

図: VLAN 構成

選択基準

VLAN ID and Name – この画面により既存VLANを再構成するか新しい VLANを生成する。

Participation – この欄によりVLANに参加させるポートを指定する。工場出荷時デフォルトは自動検出。可能な値は;

- Include/含める - このポートは常にこのVLANのメンバーです。これはIEEE 802.1Q規格に規定された登録内容と同じです。
- Exclude/除外する – このポートは決してこのVLANのメンバーではありません。これはIEEE 802.1Q規格で禁止された登録内容と同じです。
- Autodetect – ポートがGVRP経由でこのVLANに動的に登録される可能性を特定する。GVRPの要求を受け取らなければそのポートはこのVLANに参加しません。
  これはIEEE 802.1Q規格の登録標準と同等です。

Tagging – このVLANのこのポートへのタグ付け動作を選択します。工場出荷時デフォルトは「タグを付けない」です。取り得る値は;

- タグ付き – このVLANのために送信されたすべてのフレームにタグが付きます。
- タグ無し – このVLANへ送信されたすべてのフレームはタグ付けされません。

構成可能データ

VLAN ID – 新しいVLANのためにVLAN識別子を特定する。(新しいVLANを作ろうとしている場合だけこの欄へのデータ入力ができる。)

VLAN Name　VLANに名前を特定するためこのオプションの欄を使います。32(空白も含む)までの長さの英数字が使えます。デフォルトは空白、VLAN ID 1 は常にデフォルトの名前です。

VLAN Type – この欄は構成しているVLANのタイプを識別します。デフォルトVLAN(VLAN ID = 1)のタイプを変更することはできません: 常に「デフォルト」タイプです。 この画面により新しくVLANを作成すれば、そのタイプは常に「静的な」です。 はじめてGVRP登録で作成されたVLANは、「動的な」タイプになります。このプルダウンメニューによりタイプを「静的な」に変えることができます。

構成不可能なデータ

Slot/Port – どのポートがこのラインの欄と関連しているかを表示します。

Status – ポートの参加パラメータの現在の値を表示します。

コマンドボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても、新しい設定をスイッチ に保持させるには保存しなければなりません

Delete -　このVLANを削除する。 デフォルトVLANを削除することは許可されていません。

8.3.3.2　**ステータス**

このページは現在構成されたすべてのVLANのステータスを表示します。

VLAN

Config | Status | Port Config | Port Summary | Reset Config

VLAN ID	VLAN Name	VLAN Type	Slot/Port		
1	Default	Default	Encl-CB1/0/1	Encl-CB1/0/2	Encl-CB1/0/3
			Encl-CB1/0/4	Encl-CB1/0/5	Encl-CB1/0/6
			Encl-CB1/0/7	Encl-CB1/0/8	Encl-CB1/0/9
			Encl-CB1/0/10	Encl-CB1/0/11	Encl-CB1/0/12
			Encl-CB1/0/13	Encl-CB1/0/14	Encl-CB1/0/15
			Encl-CB1/0/16	Encl-CB1/0/17	Encl-CB1/0/18
			Encl-CB1/0/19	Encl-CB1/0/20	Encl-CB1/0/21
			Encl-CB1/0/22	Encl-CB1/0/23	Encl-CB1/0/24
			Encl-CB1/0/25	Encl-CB1/0/26	Encl-CB1/0/27
			Encl-CB1/0/28	Encl-CB1/0/29	Encl-CB1/0/30
			Encl-CB1/0/31	Encl-CB1/0/32	Encl-CB1/0/33
			Encl-CB1/0/34	Encl-CB1/0/35	Encl-CB1/0/36
			Encl-CB1/0/37	Encl-CB1/0/38	Encl-CB1/0/39
			Encl-CB1/0/40	Encl-CB1/0/41	Encl-CB1/0/42
			Encl-CB1/0/43	Encl-CB1/0/44	Encl-CB1/0/45
			Encl-CB1/0/46	Encl-CB1/0/47	Encl-CB1/0/48
1002	fddi-default	Static			
1003	token-ring-default	Static			
1004	fddinet-default	Static			
1005	trnet-default	Static			

図: VLAN のステータス

構成不可能なデータ

VLAN ID - VLANのVLAN識別子(VID)。 VLAN IDの範囲は 1 から 4094 です。

VLAN Name - VLANの名前。VLAN ID 1 は常に「デフォルト」と名付けられます。

VLAN Type - VLANのタイプ:

- **デフォルト(VLAN ID=1)─常に存在**
- **静的な － 構成したVLAN**
- **動的な － 静的なものへ変換しなかった、従ってGVRPが削除する可能性のある、GVRP登録で作成されたVLAN**

Slot/Port – どのポートがこのラインの欄に関連付けられているかを表示する

8.3.3.3 ポートの構成

VLAN

Config | Status | Port Config | Port Summary | Reset Config

Slot/Port: All

Port VLAN ID (1 to 4094):* 1

Acceptable Frame Types: Admit All

Ingress Filtering: Disable

Port Priority (0 to 7):* 0

* = mandatory

Apply

図：VLAN ポート構成

選択基準

Slot/Port – 表示させたいまたはデータを構成する物理インターフェイスを選択する。パラメータをすべてのポートで同じ値に設定するため「すべて」を選択する。

Acceptable Frame Types – タグ無しフレームとプライオリティタグ付きのフレームのポートによる処理方法を指定します。「VLANのみ」を選択すれば、ポートは受信するタグ無しまたはプライオリティタグ付きのフレームをすべて破棄します。「すべてを承認する」を選べばポートで受信されたタグ無しとプライオリティタグ付きのフレームは受け入れられ、このポイントのポートVLAN IDの値を割当てられます。 いずれを選んでも、VLANがタグを付けたフレームはIEEE 802.1Q VLAN規格にしたがって転送されます。工場出荷時デフォルトは「すべてを承認」です。

Ingress Filtering – ポートにタグ付きフレームの処理方法を特定する。プルダウンメニューの入口フィルタリングを有効化すれば、このポートがタグ内のVLAN IDで識別されるVLANのメンバーでない場合、タグ付きのフレームは破棄される。プルダウンメニューから無効化するを選択すれば、すべてのタグ付きのフレームは受け入れられる。工場出荷時デフォルトは無効化です。

構成可能データ

Port VLAN ID – このポートで受信されたタグ無しあるいはプライオリティタグ付きのフレームに割当てたいVLAN IDを指定します。

Port Priority – ポートに到着するタグ無しパケットへデフォルトの 802.1pプライオリティを割当てるよう特定する。

コマンドボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても新しい設定をスイッチに保持させるには 保存しなければなりません

8.3.3.4 **Port Summary**

VLAN

Config | Status | Port Config | Port Summary | Reset Config

Listing of all Ports on the Switch

Slot/Port	Port VLAN ID	Acceptable Frame Types	Ingress Filtering	Port Priority
Encl-CB1/0/1	1	Admit All	Disabled	0
Encl-CB1/0/2	1	Admit All	Disabled	0
Encl-CB1/0/3	1	Admit All	Disabled	0
Encl-CB1/0/4	1	Admit All	Disabled	0
Encl-CB1/0/5	1	Admit All	Disabled	0
Encl-CB1/0/6	1	Admit All	Disabled	0
Encl-CB1/0/7	1	Admit All	Disabled	0
Encl-CB1/0/8	1	Admit All	Disabled	0
Encl-CB1/0/9	1	Admit All	Disabled	0
Encl-CB1/0/10	1	Admit All	Disabled	0
Encl-CB1/0/11	1	Admit All	Disabled	0
Encl-CB1/0/12	1	Admit All	Disabled	0
Encl-CB1/0/13	1	Admit All	Disabled	0
Encl-CB1/0/14	1	Admit All	Disabled	0
Encl-CB1/0/15	1	Admit All	Disabled	0
Encl-CB1/0/16	1	Admit All	Disabled	0
Encl-CB1/0/17	1	Admit All	Disabled	0
Encl-CB1/0/18	1	Admit All	Disabled	0
Encl-CB1/0/19	1	Admit All	Disabled	0
Encl-CB1/0/20	1	Admit All	Disabled	0
Encl-CB1/0/21	1	Admit All	Disabled	0
Encl-CB1/0/22	1	Admit All	Disabled	0
Encl-CB1/0/23	1	Admit All	Disabled	0
Encl-CB1/0/24	1	Admit All	Disabled	0
Encl-CB1/0/25	1	Admit All	Disabled	0
Encl-CB1/0/26	1	Admit All	Disabled	0
Encl-CB1/0/27	1	Admit All	Disabled	0

図：VLAN ポートのサマリー

構成不可能なデータ

Slot/Port- スロット/ポート

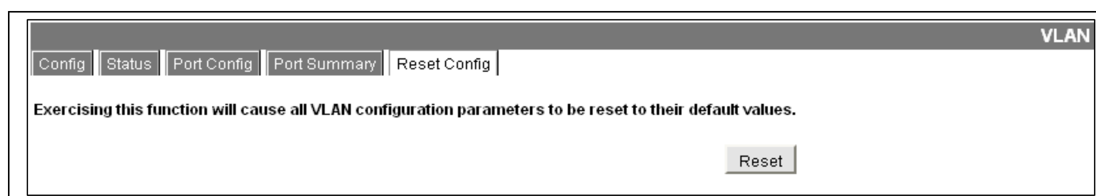
Port VLAN ID - このポートで受信されるタグ無しフレームかプライオリテ ィタグ付きフレームにこのポートが割当てるVLAN ID

Acceptable Frame Types – このポートで受信されるフレームのタイプを特定する。オプションは「VLANのみ」と「すべて許可」です。「VLANのみ」に設定されれば、このポートで受信されるタグ無しまたはプライオリティタグ付きフレームは破棄されます。「すべて許可」に設定されれば、タグ無しまたはプライオリティタグ付きのフレームは受け入れられこのポートのポートVLAN IDの値が割当てられます。どちらのオプションであっても、 VLANがタグ付けしたフレームは 802.1Q VLAN仕様にしたがって転送されます。

Ingress Filtering – 有効化すれば、このポートがフレームが関連付けられたVLANのメンバーでないなら、フレームは破棄されます。タグ付きのフレームでは、VLANはタグ内のVLAN IDで識別される。 タグ無しのフレームでは、VLANはこのフレームを受信したポートのため特定されたポートVLAN IDです。 無効にすれば、すべてのフレームは 802.1Q VLANブリッジ仕様にしたがって転送されます。工場出荷時のデフォルトは無効化です。

Port Priority – ポートに到着するタグ無しパケットへ割当てるデフォルトの 802.1pプライオリティを特定する。

8.3.3.5 **構成をリセットする**



図：VLAN 構成のリセット

コマンドボタン

Reset – このボタンを選び次の画面で選択を確認したら、すべてのVLAN の構成パラメー タは工場出荷時のデフォルト値へリセットされます。また、デフォルトVLANを除いて、すべてのVLANは削除されます。工場出荷時デフォルトは:

- すべてのオートは デフォルトVLANの 1 に割当てられる。
- すべてのポートはPVIDの 1 に構成されます。
- すべてのポートはすべてのフレームを承認する許可フレームタイプの値に構成されます。
- すべてのポートは入口フィルタリングが無効化されるように構成されます。
- すべてのポートはタグ無しのフレームだけを送信するように構成されます。
- GVRPはすべてのポート上で無効にされ、すべての動的エントリは消去されます。
- GVRPはスイッチには無効にされすべての動的エントリは消去されます。

8.3.4　　プロトコルペースのVLAN

8.3.4.1　　構成

プロトコルベースのVLANによりタグ無しパケットのフィルタリングをする判断基準を定義できます。デフォルトでは、ポート(IEEE 802.1Q)またはプロトコルベースのVLANを構成していなければ、タグ無しパケットはVLAN 1 に割当てられます。ポートベースのVLANまたはプロトコルベース のVLANまたはその両方を定義することでこの動作を無効化できます。タグ付きのパケットは常にIEEE 802.1Q標準にしたがって取り扱われ、プロトコルベースのVLANには含まれません。

ポートを特定のプロトコルのためのプロトコルベースVLANへ割当てた場合、そのポート上でそのプロトコルのために受信されたタグ無しのフレームにはプロトコルベースVLAN IDが割当てられます。他のプロトコルのためにそのポートで受信されたタグ無しのフレームにはポートVLAN IDが割当 てられます、すなわち デフォルトのPVID(1)またはポートVLAN構成画面により特にそのポートへ割当 てたPVIDです。

グループを作ることでプロトコルベースのVLANを定義します。各グループには 1 対 1 に対応するVLAN IDがあり、1 個から 3 個までのプロトコル定義を含むまたマルチプルポートを含むことができます。グループを作る場所では名前を選び、グループIDが自動的に割当てられます。

図 : プロトコルベースの VLAN 構成

選択基準

Group ID – この画面により既存プロトコルベースのVLANを再構成したり削除したり、新しいものを作ったりできます。このプルダウンメニューを使い既存PBVLANのひとつ選ぶかまたは新しいVLANを追加するため「Create」を選びます。新しいグループを作ればグループID番号が自動的に割当てられます。 128 グループまで新規作成可能です。

構成可能データ

Group Name – この欄を使い新しいグループに名前を割当てます。16 文字まで入力できます。

Protocol(s) – グループと関連付けたいプロトコルを選びます。IP、IPX、 ASPの 3 つの構成可能なプロトコルがあります。コントロールキーを押したまま 1 個以上のプロトコルを選ぶことができます。

- **IP** – IPはデータ送信のための接続無しのサービスを提供するネット ワーク・レイヤーのプロトコルです。
- **ARP** – アドレス解決プロトコル(ARP)はネットワークのレイヤーアドレスを動的に物理媒体・ アクセス制御(MAC)アドレスへマッピングする低レベルのプロトコルです。
- **IPX** – インターネットワーク・パケット・エクスチェンジ(IPX)はネット ワークでデータ を転送 するコネクションレスのデータグラム・ネットワークレイヤー・プロトコルです。

VLAN – VLANは 1 から 4094 の範囲の任意の数字が可能です。そのグループのすべてのポートはこのVLAN IDをこのグループに含めたプロトコル で受信したタグ無しパケットに割当てます。

Slot/Port – そのグループに含めるインターフェイスを選択します。ある特定のインターフェイスは特定のプロトコルのための 1 グループのみに属します。インターフェイス 0.1 をIPのグループに追加済みの場合、IPを含めた別のグループへそれを追加できません。IPXのための新しいグループへ追加することはできます。

構成不可能なデータ

Group ID – ユーザーが作成したグループを識別するために使われる番号。グループIDはグループがユーザーに作成されたときに自動的に割当てられます。

コマンドボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても新しい設定をスイッチに保持させるには 保存しなければなりません

Delete - グループIDの欄の値で識別されるプロトコルベースのVLANグループを削除します。

8.3.4.2 サマリーサマリー

Protocol-based VLAN

Config | Summary

Group Name	Group ID	Protocols	VLAN	Slot/Port

Refresh

図: プロトコルベースの VLAN サマリー

構成不可能なデータ

Group Name – そのグループに関連付けられた名前。グループ名は 16 文字まで可能です。グループの最大数は 128 です。

Group ID – グループを識別するために使われる数字。グループの作成時に自動的に割当てられました。

Protocol(s) – グループに属するプロトコル。 3 個の構成可能なプロトコルがあります: IP、IPX、 ARP。

- **IP** – IPはデータ送信のための接続無しのサービスを提供するネット ワーク・レイヤーのプロトコルです。
- **ARP** – アドレス解決プロトコル(ARP)はネットワークレイヤーを物理媒体アクセス制御 (MAC)アドレスへ動的にマッピングする低レベルのプロトコルです。
- **IPX** – インターネットワーク・パケット・エクスチェンジ(IPX)はネットワークでデータを 転送する接続無しのデータグラムのネットワークレイヤー・プロトコルです。

VLAN – グループに関連付けられたVLAN ID。

Slot/Port – グループに関連付けられたインターフェイス

コマンドボタン

Refresh - 最新の情報で画面を更新する

8.3.5 IPサブネットベースのVLAN

8.3.5.1 構成

VLANマッピングへのIPサブネットはIPサブネットからVLANテーブルのエントリを構成することにより定義されます。エントリはソースIPアドレス、ネットワークマスク、任意のVLAN ID経由により指定されます。IPサブネットからVLANの構成はデバイスのすべてのポートにより共有されます。

図：IP サブネットベースの VLAN 構成

選択基準

IP Address – VLAN IDに一意対応するIPアドレスを選択する。 別のIPサブネット・ベースのVLANを追加するには、"Add"オプションを選択してください。

構成可能データ

IP Address – VLAN IDになる有効なIPアドレスです。この欄は新しいIPサブネットベー スのVLANが作成されるときのみ構成できます。IPアドレスはドットの付いた小数点の表記法で入力。

Subnet Mask – IPアドレスの有効なサブネットマスク。この欄は新しいIP サブネットベースのVLANが作成されるときのみ構成できます。サブネットマスクはドットの付いた小数点の表記法で入力。

VLAN ID – VLAN は 1 から 4094 の範囲の任意の数が可能です。

コマンドボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても新しい設定をスイッチに保持させるには 保存しなければなりません.

Delete - IPサブネットからVLANマッピングへのエントリを削除する。

8.3.5.2 サマリー

IP Address	Subnet Mask	VLAN ID
1.2.3.4	255.255.255.0	1

図：IP サブネットベースの VLAN サマリー

構成不可能なデータ

IP Address – VLAN IDになるサブネットのIPアドレス

Subnet Mask – VLAN IDになるIPアドレスのサブネットマスク

VLAN ID - IPサブネットが利用されるVLAN IDです。 VLAN IDは 1 から 4094 の範囲の任意の数字が可能です。

コマンドボタン

Refresh - 最新の情報で画面を更新する。

8.3.6 MACベースのVLAN

8.3.6.1 構成

MACベースのVLANの機能は受信されたタグ無しパケットがVLANに割当てられ、それによりパケットのソースMACアドレスに基づくトラフィックを識別できます。

MACからVLANのマッピングはMACからVLANテーブル･エントリを構成することで定義されます。エントリはソースMACアドレスと希望のVLAN ID経由で特定されます。MACからVLAN の構成はデバイス のすべてのポートにわたって共有されます。(すなわち、MACアドレスからVLAN IDへのマッピン グを持つシステム全体の表があるということです。)

スイッチにタグ無しかプライオリティタグ付きのパケットが到着してMACからVLANテーブルにエントリがある場合、パケットのソースMACアドレスが検索されます。 エントリが見つかればそれに対応するVLAN IDがパケットに割当てられます。パケットがすでにプライオリティタグをつけられた場合、この値を維持します、くはプライオリティはゼロに設定されます。割当てられたVLAN IDはVLANテーブルで検証され、 VLANが有効化されているとパケットの入口処理は続き、それ以外の場合パケットは拒否されます。このことはユーザーがMACアドレスをシステムに作成されていないVLANへのマッピングを構成できることを意味します。

MAC-based VLAN
Config | Summary
MAC Address: Add
MAC Address :* 00:00:00:00:00:00
VLAN ID (1 to 3965) :* 0
* = mandatory
Apply

図 : MAC ベースの VLAN 構成

構成可能データ

MAC Address – VLAN IDになる有効なMACアドレスです。この欄はMACベースのVLANが作成されるときのみ構成できます。

VLAN ID - VLAN IDは 1 から 4094 の範囲の任意の数が使えます。

コマンドボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても新しい設定をスイッチに保持させるには 保存しなければなりません.

8.3.6.2　**サマリー**

MAC Address	VLAN ID
12:34:56:ab:cd:ef	1

図：MAC ベースの VLAN　サマリー

構成不可能なデータ

MAC Address - VLAN IDになるMACアドレス

VLAN ID - MACアドレスが利用されるVLAN　ID

コマンドボタン

Refresh -　スイッチの現在のデータ状態で画面のデータを更新します

8.3.7 GARP

8.3.7.1 グローバル･コンフィグ

GARP

Global Config | Port Config | Status

GVRP Mode: Disable

GMRP Mode: Disable

Apply

図 : GARP グローバル･コンフィグ



GARP の構成の変更が有効化されるには 10 秒までかかります。

選択基準

GVRP Mode – プルダウンメニューから有効化または無効化を選び、 スイッチのためのGARP VLAN登録プロトコルの管理モードを選びます。

GMRP Mode – プルダウンメニューから有効化または無効化を選択し、 スイッチの GARPマルチキャスト登録プロトコル管理モードを選びます。工場出荷時デフォルトは無効化です。

コマンドボタン

Apply - 入力した設定でスイッチを更新する。 スイッチが電源を切っても新しい設定を保持させるには保存しなければなりません。

8.3.7.2　ポートの構成

GARP

Global Config　Port Config　Status

Slot/Port: All

Port GVRP Mode: Disable

Port GMRP Mode: Disable

GARP Timers

Join Timer (centisecs) (10 to 100) :* 20

Leave Timer (centisecs) (20 to 600) :* 60

Leave All Timer (centisecs) (200 to 6000) :* 1000

* = mandatory

Apply

図: GARP　ポート構成



GARP の構成が有効化されるには最大 10 秒かかる場合があります。

選択基準

Slot/Port - データが表示または構成される物理インターフェイスを選択します。「すべて」を選ぶとすべてのポートのパラメータを設定できます。

Port GVRP Mode - プルダウンメニューから有効化または無効化を選択して GARP VLAN登録プロトコルの管理モードを選びます。無効化を選択するとプロトコルはアクティ ィブ にならず、Join時間、Leave時間、LeaveAll時間は無効です。工場出荷時デフォルトは無効化です。

Port GMRP Mode - プルダウンメニューから有効化または無効化を選択して GARP マルチキャスト登録プロトコルの管理モードを選びます。無効化するとプロトコルは アクティ ィブにならず、Join時間、Leave時間、LeaveAll時間は無効です。工場出荷時デフォルトは無効化です。

構成可能データ

Join Time (centiseconds) – GARP PDUがVLANまたはマルチキャスト グループのメンバー資格を登録(または再登録)する送信間の時間を 100 分の 1 秒単位で指定します。10 から 100 の間(0.1 から 1.0 秒)の数字を入力します。このタイマーのインスタンスは各ポートの各GARP参加者に適用されます。

Leave Time (centiseconds)– 関連するエントリを削除する前にVLAN またはマルチキャストのグループへの登録抹消要求を受信した後の待ち時間を 100 分の 1 秒単位で指定します。これは他のステーションがサービスを中断せずに維持するために同じ属性の登録を完了するまでの時間です。20 から 600(0.2 から 6.0 秒)の数字を入力します。工場出荷時デフォルトは 0.6 秒です。このタイマーのインスタンスは各ポートの各GARP参加者に適用されます。

Leave All Time (centiseconds) – LeaveAll時間はどの程度頻繁にLeaveAll PDUが行われるかを制御します。LeaveAll PDUはすべての登録が短時間に登録抹消されるかを示します。参加者は登録を維持するために再参加する必要があります。LeaveAll期間タイマーはLeaveAll時間からLeaveAll x 1.5 倍の範囲で任意に設定されます。タイマーは 100 分の 1 秒で特定されます。

200 から 6000 (2 から 60 秒)の数字を入力します。工場出荷時デフォルトは 10 秒です。このタイマーのインスタンスは各 ポートの各GARP参加者に適用されます。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。 電源を切ってもスイッチに新しい値を保持させるには保存しなければなりません。

8.3.7.3 ステータス

この画面はスイッチと個々のポートのGARPステータスを表示します。 タイマーはポートのステータスが有効化されていると表示されているときのみ該当します。

GARP

Global Config | Port Config | Status

Switch GVRP: Disabled

Switch GMRP: Disabled

Slot/Port	Port GVRP Mode	Port GMRP Mode	Join Timer (centisecs)	Leave Timer (centisecs)	Leave All Timer (centisecs)
Encl-CB1/0/1	Disabled	Disabled	20	60	1000
Encl-CB1/0/2	Disabled	Disabled	20	60	1000
Encl-CB1/0/3	Disabled	Disabled	20	60	1000
Encl-CB1/0/4	Disabled	Disabled	20	60	1000
Encl-CB1/0/5	Disabled	Disabled	20	60	1000
Encl-CB1/0/6	Disabled	Disabled	20	60	1000
Encl-CB1/0/7	Disabled	Disabled	20	60	1000
Encl-CB1/0/8	Disabled	Disabled	20	60	1000
Encl-CB1/0/9	Disabled	Disabled	20	60	1000
Encl-CB1/0/10	Disabled	Disabled	20	60	1000
Encl-CB1/0/11	Disabled	Disabled	20	60	1000
Encl-CB1/0/12	Disabled	Disabled	20	60	1000
Encl-CB1/0/13	Disabled	Disabled	20	60	1000
Encl-CB1/0/14	Disabled	Disabled	20	60	1000
Encl-CB1/0/15	Disabled	Disabled	20	60	1000
Encl-CB1/0/16	Disabled	Disabled	20	60	1000
Encl-CB1/0/17	Disabled	Disabled	20	60	1000
Encl-CB1/0/18	Disabled	Disabled	20	60	1000
Encl-CB1/0/19	Disabled	Disabled	20	60	1000
Encl-CB1/0/20	Disabled	Disabled	20	60	1000
Encl-CB1/0/21	Disabled	Disabled	20	60	1000
Encl-CB1/0/22	Disabled	Disabled	20	60	1000

図：GARP のステータス

構成不可能なデータ

Switch GVRP – スイッチのGARP VLANの登録プロトコルの管理モー ドが有効または無効かを表示します。工場出荷時デフォルトは無効化です。

Switch GMRP – このスイッチのGARPマルチキャスト登録プロトコルの管理モ ードを有効化するか無効化するかを示します。工場出荷時デフォルトは無効化です。

Slot/Port - インターフェイスのスロット/ポート。

Port GVRP Mode – ポートのGVRP管理モードを有効化する か無効化するかを示す。工場出荷時のデフォルトは無効化です。

Port GMRP Mode - ポートのGMRP管理モードを有効化する か無効化するかを示す。工場側デフォルトは無効化されている。

Join Timer (centiseconds) - GARP PDUがVLANまたはマルチキャストグループのメンバー資格を登録(または再登録)する送信間の時間を 100 分の 1 秒単位で指定します。このタイマーのインスタンスは各ポートの各GARP参加者に適用されます。許容される値は 0.1 から 1.0 秒です。工場出荷時デフォルトは 0.2 秒です。

Leave Timer (centiseconds) ― VLANまたはマルチキャストグループに対する登録抹消要求の受信後関連エントリを削除するまで待機する時間を指定します。これにより別のステーションはサービスを継続できるために同じ属性に対して登録を維持することができます。

Leave All Timer (centiseconds) - LeaveAll時間はどの程度頻繁にLeaveAll PDUが行われるかを制御します。LeaveAll PDUはすべての登録が短時間に登録抹消されるかを示します。参加者は登録を維持するために再参加する必要があります。このタイマーのインスタンスは各ポートの各GARP参加者に適用されます。LeaveAll期間タイマーはLeaveAll時間からLeaveAll x 1.5 倍の範囲で任意に設定されます。許容できる値は 2 から 60 秒です。工場出荷時デフォルトは 1000(10 秒)です。

8.3.8 VTP

8.3.8.1 構成

VTP

Config | Summary

Admin Mode: Enable

Domain Name:

Device Mode: Server

Pruning Mode: Disable

Domain Password:

V2 Mode: Disable

Page	1
Slot/Port	Trunk
All	
Encl-CB1/0/1	Disable
Encl-CB1/0/2	Disable
Encl-CB1/0/3	Disable
Encl-CB1/0/4	Disable
Encl-CB1/0/5	Disable
Encl-CB1/0/6	Disable
Encl-CB1/0/7	Disable
Encl-CB1/0/8	Disable
Encl-CB1/0/9	Disable
Encl-CB1/0/10	Disable
Encl-CB1/0/11	Disable
Encl-CB1/0/12	Disable
Encl-CB1/0/13	Disable
Encl-CB1/0/14	Disable
Encl-CB1/0/15	Disable
Encl-CB1/0/16	Disable

図：VTP 構成

選択基準

Admin Mode– VTP機能を有効化または無効化する

Device Mode – プルダウンメニューによりVTPデバイスモードを(クライアント、 サーバ、透過的から)選択する。VTPデバイスのデフォルトの運用モードは「サーバ」です。

Pruning Mode – VTPプルーニングモードを有効化または無効化します。

Trunkport – VTPのトランクポートを有効化または無効化します。

V2 Mode – VTPバージョン 2 モードを有効化または無効化します。

構成可能データ

Domain Name – VTPの管理ドメイン名を設定します。

Domain Password – VTP管理ドメインのパスワードを設定します。

コマンドボタン

Apply - 新しい構成を適用し変更を有効化します。これらの変更は構成を保存しなければ電源を切ると保持されません。

8.3.8.2　サマリー

VTP

Config | Summary

VTP Status	VTP Version	Configuration Revision	Maximum VTP supported VLANs	Support VLAN number	Operating Mode	Domain Name	Pruning Mode	V2 Mode	MD5 Digest	Configuration last modified	u
Enable	2	0	64	5	Server		Disable	Disable	0x3E 0x87 0x56 0x96 0xB2 0x7A 0xD5 0x5D	0.0.0.0 at 01-01-70 08:00:16	ir

Page	1
Slot/Port	Trunk
Encl-CB1/0/1	Disable
Encl-CB1/0/2	Disable
Encl-CB1/0/3	Disable
Encl-CB1/0/4	Disable
Encl-CB1/0/5	Disable
Encl-CB1/0/6	Disable
Encl-CB1/0/7	Disable
Encl-CB1/0/8	Disable
Encl-CB1/0/9	Disable
Encl-CB1/0/10	Disable
Encl-CB1/0/11	Disable
Encl-CB1/0/12	Disable
Encl-CB1/0/13	Disable
Encl-CB1/0/14	Disable

図：VTP　サマリー

構成不可能なデータ

VTP Status – **VTPのステータスを表示する。**

VTP Version – **スイッチで稼働しているVTPのバージョンを表示する。**

Configuration Revision – **このスイッチの現在の構成改訂番号を表示する。**

Maximum VTP supported VLANs – **ローカルでサポートされているVLANの最大数。**

Support VLAN number – **既存VLANの数。**

Operating mode – **VTPの運用モードを表示する。**

Domain Name – **スイッチの管理ドメインを識別する名前を表示する。**

Pruning mode – **VTPプルーニングモードを表示する。**

V2 Mode - VTPバージョン 2 モードを表示する。

MD5 Digest – **VTPドメインのステータスのチェックサム値を表示する。**

Configuration last modified – **最後に構成が変更されたタイムスタンプとデータベー スを変更したスイッチのIPアドレス。**

Local updater ID – **VTPドメインのステータスのローカル･アップデーターを表示する。**

Trunkport – **VTPのトランクポートを表示する。**

8.3.9 IGMP スヌーピング

8.3.9.1 構成とステータス

このメニューによりIGMPスヌーピングのパラメータを構成します。これがマルチキャスト･トラフィックの転送リストを作るのに使われます。Read･Writeアクセス特権ユーザーのみこの画面のデータを変更できます。

図：IGMP スヌーピング　構成とステータス

選択基準

管理モード - プルダウンメニューからスイッチのIGMPスヌーピングの管理モードを選択します。デフォルトは無効化です。

構成不可能なデータ

Multicast Control Frame Count – CPUに処理されるマルチキャストコントロールフレームの数

Interfaces Enabled for IGMP Snooping – 現在IGMPスヌーピングを有効化したすべてのインターフェイスのリスト

Data Frames Forwarded by the CPU – CPUに転送されるデータフレームの数

VLAN Ids Enabled For IGMP Snooping – IGMPスヌーピングを有効化したVLANのIDを表示します

コマンドボタン

Apply - 入力した数値でスイッチを更新する。電源を切っても新しい値をスイッチに保持させる には保存しなければなりません。 Read･Writeアクセス特権がある場合にのみこのボタンが見えます。

8.3.9.2 インターフェイスの構成

Snooping

Config and Status | Interface Config | VLAN Config | VLAN Status

Slot/Port: All

Admin Mode: Disable

Group Membership Interval(secs) (2 to 3600):* 260

Max Response Time(secs)(Less Than Group Membership Interval) (1 to Group Membership Interval - 1 (secs)):* 10

Multicast Router Present Expiration Time(secs) (0 to 3600):* 0

Fast Leave Admin Mode: Disable

* = mandatory

Apply

図 : IGMP スヌーピングインターフェイス・コンフィグ

選択基準

Slot/Port - 選択ボックスに物理VLANとLAGインターフェイスが記載される。構成するインターフェイスを選択します。

Admin Mode – プルダウンメニューからスイッチのIGMPスヌーピングに選ばれたインターフェイスのインターフェイス・モードを選択します。

Fast Leave Admin mode – プルダウンメニューから特定インターフェイスのためのFastLeaveモードを選択します。デフォルトは無効化です。

構成可能データ

Group Membership Interval – ある特定のインターフェイスの特定のグループがそのインターフェイスをグループから削除する前に行う通知をスイッチが待機する時間を指定します。1 から 3600 秒の値を入力します。デフォルトは 260 秒です。

Max Response Time – インターフェイスの特定グループへの通知を受け取れなかったのでインターフェイスについてクエリーを送った後スイッチが待機する時間を指定します。1 以上か 1 に等しくかつグループメンバーシップ間隔の秒数より少ない値を入力します。デフォルトは 10 秒です。構成値はグループメンバーシップの間隔より小さくなければなりません。

Multicast Router Present Expiration Time – インターフェイスのクエリーを受け取ってそれがインターフェイスのリストから削除されるまでスイッチが待機する時間を指定します。0 から 3600 秒の値を入力します。デフォルトはゼロ秒です。ゼロの値は無限のタイムアウト、すなわちタイムアウトなしを意味します。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。電源を切っても新しい値をスイッチに保持させるには保存しなければなりません。 Read・Writeアクセス特権がある場合にのみこのボタンが見えます。

8.3.9.3 VLAN構成

Snooping

Config and Status | Interface Config | VLAN Config | VLAN Status

VLAN ID: New Entry
VLAN ID (1 to 3965):*
Admin Mode: Enable
Fast Leave Admin Mode: Disable
Group Membership Interval (Max Response Time + 1 to 3600):* 260
Maximum Response Time (1 to Group Membership Interval - 1):* 10
Multicast Router Expiry Time (0 to 3600):* 0
* = mandatory
Apply Disable

図：IGMP スヌーピング VLAN 構成

選択基準

VLAN ID – IGMPスヌーピングが有効化されるVLANのIDのリストを指定します

Fast Leave Admin Mode - 特定したVLAN IDのIGMPスヌーピング･FastLeaveモードを有効化または無効化します

構成可能データ

VLAN ID – 新規のエントリがVLAN IDのコンボボックスで選ばれたとき出現します。事前に構成できるスヌーピングパラメータが設定されたVLAN IDを指定します。

Admin Mode – 特定されたVLAN IDのIGMPスヌーピングを有効化または無効化します。

Group Membership Interval – 特定されたVLAN IDのIGMPスヌーピングのグループメンバーシップの間隔値を設定します。有効な範囲は(最大応答時間 + 1) から 3600 です。

Maximum Response Time - 特定のVLAN IDのIGMPスヌーピングの最大限の応答時間の値を設定します。

Multicast Router Expiry Time – 特定のVLAN IDのIGMPスヌーピングのマルチキャストルータの終了時間の値を設定します。有効な範囲は 0 から 3600 です。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。

Disable – スイッチをデフォルト値に更新する。

8.3.9.4 **VLAN のステータス**

Snooping

Config and Status | Interface Config | VLAN Config | VLAN Status

VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval	Max Response Time	Multicast Router Expiry Time

Refresh

図：IGMP スヌーピング VLAN ステータス

構成不可能なデータ

VLAN ID – IGMPスヌーピングモードが有効なすべてのVLAN ID

Admin Mode – VLAN IDのIGMPスヌーピングモード

Fast Leave Admin Mode - VLAN IDのFastLeaveモード

Group Membership Interval – 特定のVLAN IDのIGMPスヌーピングのグループメンバーシップ間隔。有効な範囲は 2 から 3600 です。この値は最大応答時間より大きいことが必要です。

Maximum Response Time – 特定のVLAN IDのIGMPスヌーピングの応答時間の最大限値です。有効な範囲は 1 から 3599 までです。この値はグループメンバーシップの間隔値より大きいことが必要です。

Multicast Router Expiry Time – 特定のVLAN IDのIGMPスヌーピングのマルチキャストルータ終了時間。 有効な範囲は 0 から 3600 秒です。

コマンドボタン

Refresh - データベースを再取得し、テーブルの最初のエントリから改めて表示します。

8.3.10 IGMP スイッチスヌーピング･クエリア

8.3.10.1 構成

このメニューによりIGMPスヌーピングのクエリアのパラメータを構成します。Read･Writeアクセス特権のあるユーザーのみ画面のデータを変更できます。

図：IGMP スヌーピング･クエリア構成

選択基準

Snooping Querier Admin Mode – プルダウンメニューからスイッチのIGMPスヌーピングの管理モードを選択します。デフォルトは無効化です。

構成可能データ

Snooping Querier Address - 定期的なIGMPクエリーの送信元アドレスとして使うためスヌーピング･クエリア･アドレスを指定します。

IGMP Version – 定期的なIGMPクエリーに使われるIGMPプロトコルのバージョンを指定します。

Query Interval - スヌーピング･クエリアによって送られる定期的なクエリーの間の間隔を秒数で指定します。クエリー間隔は 1 から 1800 の範囲の値でなければなりません。デフォルトは 60 です。

Querier Expiry Interval – 最後のクエリア情報が削除された以降の間隔を秒数で指定します。クエリア終了間隔は 60 から 300 の範囲の値でなければなりません。デフォルトは 60 です。

コマンドボタン

Apply - 構成した値でスイッチを更新する。

Refresh - ページに情報を読み込み直します。

8.3.10.2　**VLAN構成**

図 : IGMP スヌーピング･クエリア　VLAN 構成

選択基準

VLAN ID – IGMPスヌーピング･クエリアが有効化されたVLAN IDを選択します。

Querier Election Participate Mode – 選択モードでIGMPスヌーピングクエリアを有効化または無効化します。このモードを無効化すると、VLANの同じバージョンの別のクエリアを見たときにスヌーピングクエリアは非クエリア状態に移ってしまいます。このモードが有効のときのみ、スヌーピング･クエリアは、IPアドレスがクエリアとして選択され、そのVLANでのクエリアとして稼働している場合、クエリア選択に参加できます。他方のクエリアは非クエリア状態へ移行します。

構成可能データ

VLAN ID VLAN ID選択リストで「New　Entry」が選択されたときに出現します。IGMPスヌーピング･クエリアを有効化するVLANIDを指定します。ユーザーは事前に構成できるスヌーピングクエリアのパラメータも設定できます

Snooping Querier VLAN Address - 特定のVLAN上で送られる定期的なIGMPクエリーのソースアドレスとして使われるスヌーピング･クエリア･アドレスを指定します。

コマンドボタン

Apply - 構成した値でスイッチを更新する。

Delete - 選択したVLANでスヌーピング･クエリアを無効化します。VLANが選択されていないとボタンは表示されません。

Refresh - ページに情報を読み込み直します。

8.3.10.3 VLAN 構成概要

VLAN ID	Admin Mode	Querier Election Participate Mode	Snooping Querier VLAN Address

図：IGMP スヌーピングクエリア VLAN 構成 サマリー

構成可能データ

VLAN ID Search – VLAN IDを入力し検索ボタンをクリックします。設定が存在すればその項目が表示されます。完全一致が条件です

構成不可能なデータ

VLAN ID – IGMPスヌーピングクエリアが管理上有効化されたVLAN IDを指定します。

Admin ModeスイッチのIGMPスヌーピングの管理モードを表示します。

Querier Election Participate Mode –VLANのクエリア選択参加モードを表示します。このモードを無効化すると、VLANの同じバージョンの別のクエリアを見たときにスヌーピングクエリアは非クエリア状態に移ってしまいます。このモードが有効化されている場合のみ、スヌーピング･クエリアは、IPアドレスがクエリアとして選択され、そのVLANでのクエリアとして稼働しているようなクエリア選択に参加できます。他方のクエリアは非クエリア状態へ移行します。

Snooping Querier VLAN Address - 特定のVLAN上で送られる定期的なIGMPクエリーのソースアドレスとして使われるスヌーピング･クエリア･アドレスを表示します。

コマンドボタン

Search – 特定のVLAN IDを検索します。

Refresh – 特定のVLAN IDを検索します。

8.3.10.4 VLAN ステータス

Snooping Querier

Config | VLAN Config | VLAN Config Summary | VLAN Status

VLAN ID	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time (secs)

Refresh

図：IGMP スヌーピング・クエリア VLAN ステータス

構成不可能なデータ

VLAN ID – IGMPスヌーピングクエリアが管理上有効化されておりVLANがVLANデータベースに存在するVLAN IDを指定します。

Operational State - VLANでのIGMPスヌーピングクエリアの操作状態を指定します。次の状態のどれかであるはずです:

- **Querier**-スヌーピングスイッチがVLANにあるクエリアです。スヌーピングスイッチは構成されたクエリアがクエリーする間隔に等しい間隔で定期的にクエリーを送り出します。スヌーピングスイッチがよりよいクエリアをVLANに発見した場合、非クエリアモードへ移ります。
- **Non-Querier** - スヌーピングスイッチがVLANで非クエリアモードです。クエリア終了間隔タイマーが終了すると、スヌーピングスイッチはクエリアモードへ移ります。
- **Disabled** – スヌーピングクエリアがVLAN上で稼働していません。スヌーピングクエリアはIGMPスヌーピングがVLANで稼働していないとき、または、クエリアアドレスが構成されていないかネットワーク管理アドレスも構成されていない場合、無効化されます。

Operational Version – クエリアの操作IGMPプロトコルバージョンを表示します。

Last Querier Address – クエリーがVLANでスヌープされた最後のクエリアのIPアドレスを表示します。

Last Querier Version – VLANでクエリーがスヌープされた最後のクエリアのIGMPプロトコルバージョンを表示します。

Operational Max Response Time – スヌーピングクエリアにより送られたクエリーで使われる最大応答時間を表示します。

コマンドボタン

Refresh - ページに情報を読み込み直します。

8.3.11 IGMPマルチキャスト静的グループ

8.3.11.1 構成

Multicast Static Groups

Config | Status

MAC Filter	MAC Address	VLAN ID	Slot/Port
Create Filter		1	Encl-CB1/0/1 Encl-CB1/0/2 Encl-CB1/0/3 Encl-CB1/0/4 Encl-CB1/0/5 Encl-CB1/0/6 Encl-CB1/0/7 Encl-CB1/0/8

Apply Delete

図：IGMP マルチキャスト静的グループ　構成



この機能はIGMPスヌーピングインターフェイスモードが有効化されている場合のみ動作します。

構成不可能なデータ

MAC Filter – これはすべての構成されたL2Mcastグループのための MACアドレスとVLAN IDの組み合わせのリストです。既存L2Mcastグループのポートマスクを変更するには変更するエントリを選択します。新しいL2Mcastグループを追加するには、「フィルター作成」をリストのトップから選択します。

VLAN ID – L2Mcastグループのパケットを完全に識別するMACアドレスと共に使われるVLAN ID。「Create Filter」オプションを選択した場合のみ、この欄を変更できます。

構成可能データ

MAC Address - 01:00:5E:xx:xx:xx形式のL2McastグループのMACアドレスです。「フィルター作成」オプションを選択した場合のみ、この欄を変更できます。これらMACアドレスのL2Mcastグループは定義できません:

- 00:00:00:00:00:00
- 01:00:5E:00:00:00 to 01:00:5E:00:00:FF
- FF:FF:FF:FF:FF:FF

Slot/Port - L2Mcastグループへ含めるポートをリストします。

コマンドボタン

Apply - 画面の設定をスイッチに更新します。。パワーサイクル後、設定を保持するには保存してください。

Delete - 現在選択されているL2Mcastグループを削除します。

8.3.11.2 ステータス

このパネルによりL2Mcastの静的/動的グループにあるエントリについての情報を表示します。これらの項目は受信したフレームを転送する方法を決定する透過的ブリッジングに使用されます。

Multicast Static Groups

Config | Status

VLAN	MAC Address	Slot/Port(s)	Active State

Refresh

図：IGMP マルチキャスト静的グループ・ステータス

構成不可能なデータ

VLAN ー L2McastグループのVLAN ID値。

MAC Address – スイッチが転送情報を持つマルチキャストのMACアドレスです。フォーマットは 6 バイトのMACアドレスです。たとえば、01:00:5E:00:11:11

Slot/Port – インターフェイスの数はマルチキャストグループに属します。

Active State – アクティブなインターフェイスの数はマルチキャストグループに属します。

コマンドボタン

Refresh - データベースを再取得して、テーブルの最初のエントリから再度表示を開始する。

8.3.12 マルチキャスト･ルータ

8.3.12.1 構成

Multicast Router

Config | Statistics | VLAN Config | VLAN Statistics

Slot/Port: Encl-CB1/0/1

Multicast Router: Disable

Apply

図： IGMP マルチキャストルータ 構成

選択基準

Slot/Port – 選択ボックスはすべてのスロット/ポートをリストします。マルチキャストルータを有効化するインターフェイスを選択してください。

Multicast Router – 選択されたスロット/ポートのマルチキャストルータを有効化または無効化します

コマンドボタン

Apply -入力した数値でスイッチを更新する。

8.3.12.2 統計

Multicast Router

Config | Statistics | VLAN Config | VLAN Statistics

Interface	Multicast Router
Encl-CB1/0/1	Disabled
Encl-CB1/0/2	Disabled
Encl-CB1/0/3	Disabled
Encl-CB1/0/4	Disabled
Encl-CB1/0/5	Disabled
Encl-CB1/0/6	Disabled
Encl-CB1/0/7	Disabled
Encl-CB1/0/8	Disabled
Encl-CB1/0/9	Disabled
Encl-CB1/0/10	Disabled
Encl-CB1/0/11	Disabled
Encl-CB1/0/12	Disabled
Encl-CB1/0/13	Disabled
Encl-CB1/0/14	Disabled
Encl-CB1/0/15	Disabled
Encl-CB1/0/16	Disabled
Encl-CB1/0/17	Disabled
Encl-CB1/0/18	Disabled
Encl-CB1/0/19	Disabled
Encl-CB1/0/20	Disabled
Encl-CB1/0/21	Disabled
Encl-CB1/0/22	Disabled
Encl-CB1/0/23	Disabled
Encl-CB1/0/24	Disabled
Encl-CB1/0/25	Disabled
Encl-CB1/0/26	Disabled
Encl-CB1/0/27	Disabled
Encl-CB1/0/28	Disabled

図： IGMP マルチキャストルータ統計

構成不可能なデータ

Interface – すべての物理およびLAGインターフェイスをリストします。

Multicast Router – マルチキャストルータが有効か無効であるインターフェイスを指定します。

コマンドボタン

Refresh - データベースを再取得して、テーブルの最初のエントリから始めて再表示する。

8.3.12.3 VLAN構成

Multicast Router

Config | Statistics | VLAN Config | VLAN Statistics

Slot/Port: Encl-CB1/0/1

VLAN ID (1 to 3965):* 1

Multicast Router: Disable

* = mandatory

Apply

図：IGMP マルチキャストルータ VLAN 構成

選択基準

Slot/Port – 選択ボックスはすべてのスロット/ポートをリストします。マルチキャストルータを有効化するインターフェイスを選択します。

Multicast Router – VLAN IDでは、マルチキャストルータはこれにより有効化または無効化できます。

構成可能データ

VLAN ID – マルチキャストルータモードが有効化または無効化されるVLAN ID

コマンドボタン

Apply - 入力した数値でスイッチを更新する。

8.3.12.4 VLAN 統計

Slot/Port:	Encl-CB1/0/1
VLAN ID	**Multicast Router**

Multicast Router
Config | Statistics | VLAN Config | VLAN Statistics
Refresh

図：IGMP マルチキャストルータ VLAN 統計

選択基準

Slot/Port – 選択ボックスはすべてのスロット/ポートをリストします。統計を表示するインターフェイスを選択してください。

構成不可能なデータ

VLAN ID – マルチキャストルータモードが有効化されたすべてのVLAN IDです。

Multicast Router – VLAN IDのためのマルチキャスト･ルータ･モード

コマンドボタン

Refresh - データベースを再取得して、テーブルの最初のエントリから改めて表示します。

8.3.13 MLD スヌーピング

8.3.13.1 構成とステータス

このメニューによりMLDスヌーピングのパラメータを構成します、これはマルチキャストトラフィックの転送リストを作るのに使われます。 Read･Writeアクセスの特権ユーザーのみ画面データを変更できます。

Snooping
Config and Status | Interface Config | VLAN Config | VLAN Status
Admin Mode: Disable
Multicast Control Frame Count: 0
Interfaces Enabled for MLD Snooping: [None]
Data Frames Forwarded by the CPU: 0
VLAN Ids Enabled for MLD Snooping:

図：MLD スヌーピング 構成とステータス

選択基準

Admin Mode - プルダウンメニューからスイッチのMLDスヌーピングの管理モードを選択します。デフォルトは無効化です。

構成不可能なデータ

Multicast Control Frame Count – CPUに処理されるマルチキャストコントロールフレームの数

Interfaces Enabled for MLD Snooping – 現在MLDスヌーピングが有効化されたすべてのインターフェイスのリスト。

Data Frames Forwarded by the CPU – CPUに転送されるデータフレームの数

VLAN Ids Enabled For MLD Snooping – MLDスヌーピングが有効化されたVLAN IDを表示します。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。電源を切っても新しい値をスイッチに保持させるには保存しなければなりません。 Read･Writeアクセス特権がある場合にのみこのボタンが見えます。

8.3.13.2　インターフェイスの構成

図 : MLD スヌーピングインターフェイス

選択基準

Slot/Port - 選択ボックスに物理VLANとLAGインターフェイスが記載される。構成するインターフェイスを選択します。

Admin Mode – プルダウンメニューからスイッチがMLDスヌーピングの選択されたインターフェイスのためにインターフェイスモードを選択します。デフォルトは無効化です。

Fast Leave Admin mode – プルダウンメニューから特定インターフェイスのためのFastLeaveモードを選択します。デフォルトは無効化です。

構成可能データ

Group Membership Interval – 特定のインターフェイスの特定のグループへの通知をそのグループからそのインターフェイスを削除するまでスイッチに待たせる時間を指定します。有効な範囲は 2 から 3600 秒です。構成された値は最大応答時間より大きくなければなりません。デフォルトは 260 秒です。

Max Response Time – あるインターフェイスのクエリー送信の完了後、そのインターフェイスの特定のグループへの通知が受信されなかった場合、スイッチの待機時間を指定します。1 より大きいか 1 に等しくかつグループメンバーシップの間隔より小さい秒数の値を入力します。デフォルトは 10 秒です。構成値はグループメンバーシップの間隔よりも小さくなければなりません。

Multicast Router Present Expiration Time –マルチキャストルータが付いたインターフェイスのリストからそれを削除する前に、あるインターフェイスのクエリーを受け取るためスイッチが待機する時間を指定します。0 と 3600 秒の間の値を入力します。デフォルトは 0 秒です。ゼロの値は無期限を示します。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。電源を切っても新しい値をスイッチに保持させるには保存しなければなりません。 Read・Writeアクセス特権がある場合にのみこのボタンが見えます。

8.3.13.3　VLAN 構成

図：MLD スヌーピング VLAN 構成

選択基準

VLAN ID – MLDスヌーピングが有効化されたVLAN IDのリストを指定します。

Fast Leave Admin Mode – 特定のVLAN IDのMLDスヌーピング･FastLeaveモードを有効化または無効化します。

構成可能データ

VLAN ID – VLAN

IDコンボボックスに｢New Entry｣が選択されたときに出現します。事前に構成できるスヌーピングパラメータが設定されるVLAN IDを指定します。

Group Membership Interval – 特定のVLAN IDのMLDスヌーピングのグループメンバーシップの間隔の値を設定します。有効な範囲は(最大応答時間 + 1) から 3600 です。

Maximum Response Time – 特定のVLAN IDのMLDスヌーピングの最大応答時間の値を設定します。有効な範囲は 1 から (グループメンバーシップ間隔 - 1) です。この値はグループメンバーシップの間隔の値より小さくなければいけません。

Multicast Router Expiry Time – 特定のVLAN IDのMLDスヌーピングのマルチキャストルータ終了時間の値を設定します。有効な値は 0 から 3600 です。

構成不可能なデータ

Admin Mode – 特定のVLAN IDのMLDスヌーピングモードです。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。

Disable – デフォルトの値でスイッチを更新する。

8.3.13.4 VLAN ステータス

Snooping

Config and Status | Interface Config | VLAN Config | VLAN Status

VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval (secs)	Max Response Time (secs)	Multicast Router Expiry Time (secs)

Refresh

図：MLD スヌーピング VLAN ステータス

構成不可能なデータ

VLAN ID – MLDスヌーピングモードが有効化されたすべてのVLAN ID。

Admin Mode – VLAN IDのMLDスヌーピングモード。

Fast Leave Admin Mode – VLAN IDのためのFastLeaveモード。

Group Membership Interval – 特定のVLAN IDのMLDスヌーピングのグループメンバーシップ間隔。 有効な範囲は 2 から 3600 です。

Maximum Response Time – 特定のVLAN IDのMLDスヌーピングの最大応答時間。有効な範囲は 1 から 3599 です。この値はグループメンバーシップの間隔値より大きいことが必要です。

Multicast Router Expiry Time – 特定のVLAN IDのためのMLDスヌーピングのマルチキャストルータの終了時間。有効な範囲は 0 から 3600 です。

コマンドボタン

Refresh - データベースを再取得してテーブルの最初のエントリから改めて表示します。

8.3.14 MLD スヌーピング･クエリア

8.3.14.1 構成

このメニューによりMLDスヌーピング･クエリアのパラメータを構成します。Read･Writeアクセス特権ユーザーのみ画面のデータを変更できます。

Snooping Querier	
Config / VLAN Config / VLAN Config Summary / VLAN Status	
Snooping Querier Admin Mode:	Disable
Snooping Querier Address :*	:: Supported Formats
MLD Version:	1
Query Interval(secs) (1 to 1800):*	60
Querier Expiry Interval(secs) (60 to 300):*	60
* = mandatory	
	Apply Refresh

図：MLD スヌーピング･クエリア構成

選択基準

Snooping Querier Admin Mode – プルダウンメニューからスイッチのMLDスヌーピングの管理モードを選択します。デフォルトは無効化です。

構成可能データ

Snooping Querier Address – 定期的なMLDクエリーのソースアドレスとして使われるスヌーピングクエリアアドレスを指定します。このアドレスはクエリーが送られるVLANにアドレスが構成されていないときに使われます。

MLD Version – 定期的なMLDクエリーに使われるMLDプロトコルのバージョンを指定します。

Query Interval - スヌーピング･クエリアによって送られる定期的なクエリーの間の間隔を秒数で指定します。クエリー間隔は 1 から 1800 の範囲の値でなければなりません。デフォルトは 60 です。

Querier Expiry Interval – 最後のクエリア情報が削除された以降の間隔を秒数で指定します。クエリア終了間隔は 60 から 300 の範囲の値でなければなりません。デフォルトは 60 です。

コマンドボタン

Apply - 構成した値でスイッチを更新する。

Refresh - ページに情報を読み込み直します。

8.3.14.2 VLAN構成

Snooping Querier
Config | VLAN Config | VLAN Config Summary | VLAN Status
VLAN ID: New Entry
VLAN ID (1 to 3965):*
Querier Election Participate Mode: Disable
Snooping Querier VLAN Address:* Supported Formats
* = mandatory
Apply Refresh

図：MLD スヌーピングクエリア VLAN 構成

選択基準

VLAN ID – MLDスヌーピング･クエリアが有効化されたVLAN IDを選択します

Querier Election Participate Mode –MLDスヌーピング･クエリアの選択モードへの参加を有効化または無効化します。このモードを無効化すると、VLANの同じバージョンの別のクエリアを見たときにスヌーピングクエリアは非クエリア状態に移ります。このモードが有効化されている場合のみ、スヌーピング･クエリアは、IPアドレスがクエリア選択に勝ちそのVLANでのクエリアとして稼働しているクエリア選択に参加できます。他方のクエリアは非クエリア状態へ移行します。

構成可能データ

VLAN ID – VLAN ID選択リストで｢新規エントリ｣が選択されると現れます。MLDスヌーピングクエリアが有効化されるべきVLAN IDを指定します。ユーザーは事前に構成できるスヌーピングクエリアのパラメータもセットできます。

Snooping Querier VLAN Address -特定のVLANで送られる定期的なMLDクエリーのソースアドレスとして使われるスヌーピング･クエリア･アドレスを指定します。

コマンドボタン

Apply - 構成した値でスイッチを更新する。

Delete - 選択したVLANでスヌーピング･クエリアを無効化します。VLANが選択されていないとボタンは見えません。

Refresh - ページに情報を読み込み直します。

8.3.14.3 VLAN 構成概要

Snooping Querier

Config | VLAN Config | VLAN Config Summary | VLAN Status

VLAN ID Search: 0 Search

VLAN ID	Admin Mode	Querier Election Participate Mode	Snooping Querier VLAN Address

Refresh

図：MLD スヌーピングクエリア VLAN 構成概要

構成可能データ

VLAN ID Search – VLAN IDを入力し検索ボタンをクリックします。設定が存在すればその項目が表示されます。完全一致が条件です。

構成不可能なデータ

VLAN ID – MLDスヌーピングクエリアが管理上有効化されたVLAN IDを指定します。

Admin Modeー スイッチにMLDスヌーピングのための管理モードを表示します。

Querier Election Participate Mode -

VLANのクエリア選択参加モードを表示します。このモードを無効化すると、VLANの同じバージョンの別のクエリアを見たときにスヌーピングクエリアは非クエリア状態に移ります。このモードが有効化されている場合のみ、スヌーピング・クエリアは、IPアドレスがクエリアとして選択され、そのVLANでのクエリアとして稼働しているようなクエリア選択に参加できます。他方のクエリアは非クエリア状態へ移行します。

Snooping Querier VLAN Address -特定のVLANで送られる定期的なMLDクエリーのソースアドレスに使われるスヌーピング・クエリア・アドレスを表示します。

コマンドボタン

Search – 特定のVLAN IDを検索します。

Refresh - ページに情報を読み込み直します。

8.3.14.4 VLAN ステータス

Snooping Querier

Config | VLAN Config | VLAN Config Summary | VLAN Status

VLAN ID	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time (secs)

Refresh

図：MLD スヌーピング・クエリア VLAN ステータス

構成不可能なデータ

VLAN ID – MLDスヌーピングクエリアが管理上有効化されておりVLANがVLANデータベースに存在するようなVLAN IDを指定します。

Operational State – VLANでのMLDスヌーピング・クエリアの稼働状態を指定します。それは次のうちのどれかであるはずです。

- **Querier -** スヌーピングスイッチがVLANにあるクエリアです。スヌーピングスイッチは構成されたクエリアがクエリーする間隔に等しい間隔で定期的にクエリーを送り出します。スヌーピングスイッチがよりよいクエリアをVLANに発見した場合、非クエリアモードへ移ります。
- **Non-Querier -** スヌーピングスイッチがVLANで非クエリアモードです。クエリア終了間隔タイマーが終了すると、スヌーピングスイッチはクエリアモードへ移ります。
- **Disabled -** スヌーピングクエリアがVLAN上で稼働していません。スヌーピングクエリアはMLDスヌーピングがVLANで稼働していない場合、または、クエリアアドレスが構成されていないかネットワーク管理アドレスも構成されていない場合、無効化されます。

Operational Version - クエリアの操作MLDプロトコルバージョンを表示します。

Last Querier Address - クエリーがVLANでスヌープされた最後のクエリアのIPアドレスを表示します。

Last Querier Version - VLANでクエリーがスヌープされた最後のクエリアのMLDプロトコルバージョンを表示します。

Operational Max Response Time – スヌーピングクエリアにより送られたクエリーで使われる最大応答時間を表示します。

コマンドボタン

Refresh - ページに情報を読み込み直します。

8.3.15 MLDマルチキャスト静的グループ

8.3.15.1 構成

Multicast Static Groups

Config | Status

MAC Filter	MAC Address	VLAN ID	Slot/Port
Create Filter		1	Encl-CB1/0/1 Encl-CB1/0/2 Encl-CB1/0/3 Encl-CB1/0/4 Encl-CB1/0/5 Encl-CB1/0/6 Encl-CB1/0/7 Encl-CB1/0/8

Apply | Delete

図：MLD マルチキャスト静的グループ　構成



この機能はIGMP　MLDスヌーピングインターフェイスモードが有効化されている場合のみ有効です。

選択基準

MAC Filter – これはすべての構成されたL2Mcastグループのための MACアドレスとVLAN IDの組み合わせのリストです。既存L2Mcastグループのポートマスクを変更するには変更するエントリを選択します。新しいL2Mcastグループを追加するには、「フィルター作成」をリストのトップから選択します。

VLAN ID – L2Mcastグループのパケットを完全に識別するMACアドレスと共に使われるVLAN IDです。「フィルター作成」オプションを選択した場合のみ、この欄を変更できます。

構成可能データ

MAC Address - 01:00:5E:xx:xx:xx形式のL2McastグループのMACアドレスです。「フィルター作成」オプションを選択した場合のみ、この欄を変更できます。これらMACアドレスのL2Mcastグループを定義するこはできません:

- 00:00:00:00:00:00
- 33:33:00:00:00:00 to 33:33:00:00:00:FF
- FF:FF:FF:FF:FF:FF

Slot/Port - L2Mcastグループへ含めるポートをリストします。

コマンドボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても新しい設定をスイッチに保持させるには 保存しなければなりません。

Delete - 現在選択されているL2Mcastグループを削除します。

8.3.15.2 ステータス

このパネルによりL2Mcastの静的/動的グループにあるエントリについての情報を表示します。これらの項目は受信したフレームを転送する方法を決定するトランスペアレントブリッジングに使用されます。

Multicast Static Groups

Config | Status

VLAN	MAC Address	Slot/Port(s)	Active State

Refresh

図：MLD スヌーピングマルチキャスト静的グループ ステータス

構成不可能なデータ

VLAN - L2McastグループのVLAN ID値。

MAC Address - スイッチが転送情報を持つマルチキャストのMACアドレスです。フォーマットは 6 バイトのMACアドレスです。たとえば、33:33:00:00:11:11.

Slot/Port – インターフェイスの数はマルチキャストグループに属します。

Active State – アクティブなインターフェイスの数はマルチキャストグループに属します。

コマンドボタン

Refresh - データベースを再取得して、テーブルの最初のエントリから始めて再表示する。

8.3.16 MLDマルチキャスト･ルータ

8.3.16.1 構成

Multicast Router	
Config / Statistics / VLAN Config / VLAN Statistics	
Slot/Port:	Encl-CB1/0/1
Multicast Router:	Disable
	Apply

図：MLD スヌーピングマルチキャストルータ 構成

選択基準

Slot/Port – 選択ボックスはすべてのスロット/ポートをリストします。マルチキャストルータを有効化したインターフェイスを選択します。

Multicast Router – 選択したスロット/ポートのマルチキャストルータを有効化または無効化します。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。

8.3.16.2　統計

Multicast Router

Config | Statistics | VLAN Config | VLAN Statistics

Slot/Port: Encl-CB1/0/1
Multicast Router: Disable

Refresh

図：MLD スイッチヌーイングマルチキャストルータ　統計

選択基準

Slot/Port　－　1 個の選択ボックスがすべての物理インターフェイスとLAGインターフェイスをリストアップします。ステータスを表示したいインターフェイスを選択してください。

構成不可能なデータ

Multicast Router – 選択されたインターフェイスでマルチキャストルータを有効化するか無効化するかを指定します。

コマンドボタン

Refresh - データベースを再取得し、テーブルの最初のエントリから改めて表示します。

8.3.16.3 VLAN構成

Multicast Router
Config | Statistics | VLAN Config | VLAN Statistics
Slot/Port: Encl-CB1/0/1
VLAN ID (1 to 3965):* 1
Multicast Router: Disable
* = mandatory
Apply

図：MLD スヌーピングマルチキャストルータ VLAN 構成

選択基準

Slot Port – 選択リストはすべてのスロット/ポートをリストします。マルチキャストルータを有効化するインターフェイスを選択します。

Multicast Router – VLAN IDには、これによりマルチキャストルータは有効化または無効化されます。

構成可能データ

VLAN ID – マルチキャストルータ·モードが有効化または無効化されるVLAN IDです。

コマンドボタン

Apply - 入力した数値でスイッチを更新する。

8.3.16.4 **VLANの統計**

Slot/Port	Encl-CB1/0/1
VLAN ID	Multicast Router

Multicast Router — Config | Statistics | VLAN Config | VLAN Statistics — Refresh

図：MLD スヌーピングマルチキャストルータ VLAN の統計

選択基準

Slot/Port – 選択ボックスはすべてのスロット/ポートをリストします。ステータスを表示するインターフェイスを選択します。

構成不可能なデータ

VLAN ID – マルチキャストルータモードが有効なすべてのVLAN ID

Multicast Router – VLAN IDのためのマルチキャストルータ･モード

コマンドボタン

Refresh - データベースを再取得し、テーブルの最初のエントリから改めて表示します。

8.3.17　ユニキャスト･転送データベース

8.3.17.1　MFDBテーブル

マルチキャスト転送データベースはすべてのアクティブなマルチキャストアドレスエントリのためのポートのメンバー資格の情報を持っています。項目キーはVLAN IDとMACアドレスのペアから構成されます。エントリは 1 つ以上のプロトコルのデータを含んでいます。

Multicast Forwarding Database

MFDB Table | GMRP Table | IGMP Snooping Table | MLD Snooping Table | Statistics

MAC Address: [ ] Search

MAC Address	Component	Type	Description	Slot/Port	Forwarding Slot/Port(s)

Refresh

図 ： マルチキャスト転送データベース MFDB テーブル

構成可能データ

MAC Address – MFDBテーブル･エントリを表示するVLAN IDとMACアドレスの組み合わせを入力します。 2 桁の 16 進数を 8 つコロンで区切って入力します。たとえば、00:01:23:43:45:67:89:AB では最初の 2 つの 2 桁の 16 進数はVLAN ID、残りの数字がMACアドレスです。次に｢検索｣ボタンをクリックします。 アドレスが存在すれば、エントリは表示されます。 完全一致が条件です。

構成不可能なデータ

MAC Address – データを要求したマルチキャストMACアドレス。

Component – これがマルチキャスト転送データベースのこのエントリを担当すコンポーネントです。可能な値はIGMPスヌーピング、GMRPと静的フィルタリングです。

Type – これはエントリのタイプです。静的なエントリはエンドユーザーによって構成されるものです。 動的な項目の学習手順やプロトコルの結果としてテーブルに追加されます。

Description – このマルチキャストテーブル･エントリを文章で解説したものです。可能な値は構成される管理、構成されるネットワーク、と支援されるネットワークです。

Slot/Port(s) -選択されたアドレスの転送とフィルタリングに指定されたインターフェイスのリストです。

Forwarding Slot/Port(s) – 転送インターフェイスの結合と削除を静的なフィルタリングのインターフェイスとして記載されている転送リストとして表示しています。

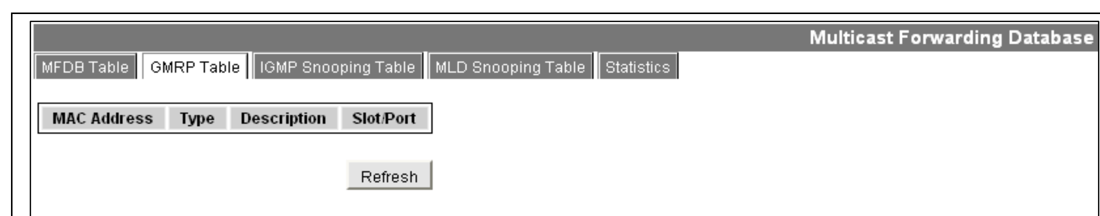
コマンドボタン

Search – MFDBデータベースのエントリをVLAN IDとMACアドレスの組み合わせで検索します。

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.3.17.2 **GMRPテーブル**

画面はGARPマルチキャスト登録プロトコルのためにに作成されたマルチキャスト転送データベースのエントリをすべて表示します。



図： マルチキャスト転送データベース GMRP テーブル

構成不可能なデータ

MAC Address - スイッチが転送またはフィルタリングの情報を持つVLAN IDとマルチキャストMACアドレスの組み合わせです。形式は 8 つの 2 桁の 16 進法の数字でコロンで区切られた、たとえば 00:01:23:45:67:89:AB:CDのようなものです。

Type – これはエントリのタイプです。静的なエントリはエンドユーザーによって構成されるものです。 動的な項目は習得の手順やプロトコルの結果としてテーブルに追加されます。

Description – このマルチキャストテーブル・エントリを表したものです。可能な値は構成される管理、構成され るネッ トワーク、支援されるネットワークを示します。

Slot/Port(s) – 選択されたアドレスの転送(Fwd:)とフィルタリング(Flt:)に 指定されたインターフ ェイスのリストです。

コマンドボタン

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.3.17.3 IGMP スヌーピングテーブル

Multicast Forwarding Database

MFDB Table | GMRP Table | IGMP Snooping Table | MLD Snooping Table | Statistics

MAC Address	Type	Description	Slot/Port

Refresh　Clear Entries

図 : マルチキャスト転送データベース IGMP スヌーピングテーブル

構成不可能なデータ

MAC Address - スイッチが転送またはフィルタリングの情報を持つVLAN IDとマルチキャストMACアドレ スの組み合わせです。形式は 8 つの 2 桁の 16 進法の数字でコロンで区切られた、たとえば 00:01:23:45:67:89:AB:CDのようなものです。

Type – これはエントリのタイプです。静的なエントリはエンドユーザーによって構成されるものです。 動的な項目は習得の手順やプロトコルの結果としてテーブルに追加されます。

Description – このマルチキャストテーブル･エントリを表したものです。可能な値は構成される管理、構成され るネッ トワーク、支援されるネットワークを示します。

Slot/Port(s)– 選択されたアドレスの転送(Fwd:)とフィルタリング(Flt:)に指定されたインターフェイスのリストです。

コマンドボタン

Clear Entries – このボタンをクリックするとIGMPスヌーピングコンポーネン トにマルチキャスト転送データベースからすべてのエントリを削除するよう命令します。

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.3.17.4　**MLDスヌーピングテーブル**

MAC Address	Type	Description	Slot/Port

Multicast Forwarding Database

MFDB Table | GMRP Table | IGMP Snooping Table | MLD Snooping Table | Statistics

Refresh　Clear Entries

図 ： マルチキャスト転送データベースの MLD スヌーピングテーブル

構成不可能なデータ

MAC Address - スイッチが転送またはフィルタリングの情報を持つVLAN IDとマルチキャストMAC アドレスの組み合わせです。形式は 8 つの 2 桁の 16 進数でコロンで区切られた 00:01:23:45:67:89:AB:CDの形式です。

Type – これはエントリのタイプです。静的なエントリはエンドユーザーによって構成されます。動的項目は習得 の手順やプロトコルの結果としてテーブルに追加されます。

Description – このマルチキャストテーブル･エントリを表したものです。可能な値は構成される管理、構成され る ネッ トワーク、支援されるネットワークを示します。

Slot/Port(s) – 選択されたアドレスの転送(Fwd:)とフィルタリング(Flt:)に指定されたインターフェイスのリストです。

コマンドボタン

Clear Entries – このボタンをクリックするとIGMPスヌーピングコンポーネントにマルチキャスト転送 データベースからすべてのエントリを削除するよう命令します。

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.3.17.5 **統計**

Multicast Forwarding Database

MFDB Table | GMRP Table | IGMP Snooping Table | MLD Snooping Table | Statistics

Max MFDB Table Entries: 256

Most MFDB Entries Since Last Reset: 0

Current Entries: 0

Refresh

図 ： マルチキャスト転送データベースの統計

構成不可能なデータ

Max MFDB Table Entries – マルチキャスト転送データベーステーブルが保持できるMFDBテーブル･エントリの最大限数

Max MFDB Table Entries – 最後のリセット以降マルチキャスト転送データベーステーブルに存在したエントリの最大数。この値はMFDBピーク値として周知です。

Current Entries: マルチキャスト転送データベーステーブルにある現在のエントリの数

コマンドボタン

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.3.18 ポート·チャネル

8.3.18.1 構成

Port Channel

Config | Status

Port Channel Name: Create App

Slot/Port	Port Channel Name	Link Trap	Administrative Mode	Static Capability Mode	Link Status	STP Mode	Load Balanc
		Enable	Enable	Disable		Disable	Source MAC address

Page		1
Slot/Port	Participation	Membership Conflicts
Encl-CB1/0/1	Exclude	
Encl-CB1/0/2	Exclude	
Encl-CB1/0/3	Exclude	
Encl-CB1/0/4	Exclude	
Encl-CB1/0/5	Exclude	
Encl-CB1/0/6	Exclude	
Encl-CB1/0/7	Exclude	
Encl-CB1/0/8	Exclude	
Encl-CB1/0/9	Exclude	
Encl-CB1/0/10	Exclude	
Encl-CB1/0/11	Exclude	
Encl-CB1/0/12	Exclude	
Encl-CB1/0/13	Exclude	
Encl-CB1/0/14	Exclude	
Encl-CB1/0/15	Exclude	
Encl-CB1/0/16	Exclude	
Encl-CB1/0/17	Exclude	
Encl-CB1/0/18	Exclude	
Encl-CB1/0/19	Exclude	

図： ポート·チャネル·コンフィグ

選択基準

Port Channel Name - この画面で既存のポートチャネルを再構成するまたは新たなポートチャネルを生成できる。このプルダウン·メニューから既存ポート·チャネルを選択する、または'Create'を選択して新ポート·チャネルを追加できる。 最大 64 個のポート·チャネルまで可能である。

Link Trap- リンク·ステータスの変化時にトラップを送らせるかを指定する。 工場側デフォルトは有効化されており、トラップは送られる。

Admin Mode - プルダウン·メニューから有効化または無効化を選択する。 ポート·チャネルが無効化されているときは、トラフィックは起こらず、LACPDUは落とされるが、ポート·チャネルを構成するリンクは解放されない。 デフォルト設定は有効化されている。

Static Capability Mode- プルダウン·エントリ欄で対応行を選択して有効化または無効化できる。 工場側デフォルトは無効化されている。 この欄はRead Onlyのユーザーには構成できない。

STPモード – ポートチャンネルと関連されたスパニングツリープロトコルの管理モードです。

- **無効化** – スパニングツリーがポートチャンネルに対し無効化される
- **有効化** – スパニングツリーがポートチャンネルに対し有効化される

Load Balance- インターフェイス・ポート・チャネルに負荷分散モードを構成する。 とりうる値:

- Source MAC address- モードを送信元MACアドレスに設定する 。
- Destination MAC address- モードを送信先MACアドレスに設定する 。
- Source and destination MAC address- モードを送信元と送信先MACアドレスに設定する。
- Source IP address- モードを送信元IPアドレスに設定する。
- Destination IP address- モードを送信先IPアドレスに設定する 。
- Source and destination IP address- モードを送信元と送信先IPアドレスに設定する 。

Participation -ポート毎にポート・チャネルのメンバーにするかを指定する。 デフォルトはexclude/除外である。 ポート・チャネルには最大 8 ポートまで割当てることができる。

構成可能データ

Port Channel Name - ポート・チャネルに割当てる名前を入力する。 最大 15 文字の英数字からなるお好きな文字列を入力できる。 有効な名前はポート・チャネル生成のために必ず指定すること。

構成不可能なデータ

Slot/Port - 構成されるポート・チャネルのスロット/ポート識別。 この欄は新ポート・チャネル生成の際は表示されない。

Link Status- リンクがアップかダウンかを示す。

Port Channel Members - スロット/ポート形式による ポート・チャネル・メンバーのリスト。

Membership Conflicts - すでに他のポート・チャネル・メンバー であるポートを示す。1 個のポートは同時に 1 個のみのポート・チャネル・メンバーになれる。このエントリが空白であれば、そのポートはどのポート・チャネルのメンバーでもない。

コマンド・ボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても新しい設定をスイッチに保持させるには 保存しなければなりません

Delete - 現在選択されている構成されたポート・チャネルを削除する。 このポート・チャネルのメンバーであったすべてのポートはポート・チャネルから削除され、デフォルトVLANに含まれる。 この欄は新ポート・チャネル生成の際は表示されない。

Refresh - スイッチの現在のデータ状態で画面のデータを更新します。

8.3.18.2　ステータス

Port Channel

Config | Status

Port Channel	Port Channel Name	Port Channel Type	Admin Mode	Static Capability Mode	Link State	STP Mode	Link Trap	Configured Ports	Active Ports	Load Balance

図： ポート·チャネル·ステータス

構成不可能なデータ

Port Channel - ポート·チャネルのスロット/ポート識別。

Port Channel Name - ポート·チャネルの名前。

Port Channel Type·タイプ - このポート·チャネルのタイプ。

Admin Mode - ポート·チャネルの管理モード、有効化または無効化である。

Static Capability Mode- ポート·チャネルの静的機能モード、有効化または無効化である。

Link Status- リンクがアップかダウンかを示す。

STPモード – ポートチャンネルと関連されたスパニングツリープロトコルの管理モードです。

- 無効: スパニングツリーがポートチャンネルに対し無効化される
- 有効 – スパニングツリーがポートチャンネルに対し有効化される

Link Trap- リンク·ステータスの変化時にトラップを送るかを指定する。 デフォルト設定は有効化されている。

Configured Ports - スロット/ポート形式によるポート·チャネルのメンバーであるポートのリスト。 ポート·チャネルには最大 8 ポートまで割当てることができる。

Active Ports - スロット/ポート形式によるポート·チャネルのアクティブに参加するメンバーであるポートのリスト。ポート·チャネルには最大 8 ポートまで割当てることができる。

インターフェイス·ポート·チャネルに負荷分散モードを構成する。 とりうる値:

- Source MAC address/送信元MACアドレス - モードを送信元MACアドレスに設定する 。
- Destination MAC address/送信先MACアドレス - モードを送信先MACアドレスに設定する 。
- Source and destination MAC address/送信元とターゲットMACアドレス - モードを送信元と送信先MACアドレスに設定する 。
- Source IP address/送信元IPアドレス - モードを送信元IPアドレスに設定する 。
- Destination IP address/送信先IPアドレス - モードを送信先IPアドレスに設定する。
- Source and destination IP address- モードを送信元と送信先IPアドレスに設定する。
- Source and destination IP address - モードを送信元と送信先IPアドレスに設定する。

8.3.19 スパニング·ツリー

8.3.19.1 スイッチ構成/ステータス

Spanning Tree

Switch Config/Status | CST | MST | CST Port | MST Port | Statistics

Spanning Tree Admin Mode: Enable
Spanning Tree Forward BPDU: Enable
Force Protocol Version : IEEE 802.1s(MSTP)
Configuration Name:* DEFAULT
Configuration Revision Level (0 to 65535) :* 0
Configuration Digest Key : 0xac36177f50283cd4b83821d8ab26de62
* = mandatory

Apply Refresh

MST ID	VID	FID
CST	1 1002 1003 1004 1005	1 1002 1003 1004 1005

図 : スパニングツリー　スイッチ

選択基準

Spanning Tree Mode – スイッチでスパニングツリーの運用が有効化されているかを指定します。値は有効化または無効化です。

Spanning Tree Forward BPDU – スイッチでスパニングツリー転送BPDUがスイッチ上で有効化されているかを指定します。値は有効化または無効化です。

Force Protocol Version – スイッチのフォース·プロトコルバージョンのパラメータを指定します。 オプションは、IEEE 802.1d, IEEE 802.1w と IEEE 802.1s です。

Force Protocol Version – スイッチ上でエッジポートBPDUフィルターを有効化するかどうか指定します。 値は有効か無効でs。

Edgeport BPDU Guard - BPDUガードをスイッチ上で有効化するかどうか指定します。値は有効か無 効です。

Uplink Fast – アップリンクファーストをスイッチ上で有効化するかどうか指定します。値は有効化 または無効化です。

構成可能データ

構成名 – 現在使われている構成を識別するため使われる識別子。 32 個までの英数字が可能です。

構成改訂レベル -現在使われている構成を識別するため使われる識別子。許可範囲は 0 から 65535 までであり、デフォルト値は 0 です。

構成不可能なデータ

Configuration digest key -現在使われている構成の識別子。

MST Table – MSTのインスタンス(CSTを含む)と個別に関連付けられた対応VLAN IDから構成されるテーブル。

VID Table – VLAN IDとそれぞれに関連付けられた対応FIDから構成されるテーブル。

FID Table – FIDとそれぞれに関連付けられた対応するVLAN IDから構成されるテーブル。

コマンドボタン

Apply - 新しい構成を適用し変更を有効化します。これらの変更は構成を保存しなければ電源を切ると保持されません。

Refresh - 最新データで更新します。

8.3.19.2 **CST**

Spanning Tree

Switch Config/Status | CST | MST | CST Port | MST Port | Statistics

Bridge Priority (0 to 61440) :*	32768
Bridge Max Age (secs) (6 to 40) :*	20
Bridge Hello Time (secs) (1 to 10) :*	2
Bridge Forward Delay (secs) (4 to 30) :*	15
Spanning Tree Maximum Hops (1 to 127) :*	20
Bridge Identifier:	80:00:00:23:8b:17:7b:85
Time Since Topology Change:	0 day 3 hr 45 min 6 sec
Topology Change Count:	0
Topology Change:	False
Designated Root:	80:00:00:23:8b:17:7b:85
Root Path Cost:	0
Root Port:	00:00
Max Age (secs):	20
Forward Delay (secs):	15
Hello Time:	2
Hold Time (secs):	3
CST Regional Root:	80:00:00:23:8b:17:7b:85
CST Path Cost:	0

* = mandatory

Apply Refresh

図 ： スパニングツリーCST 構成

構成可能データ

Bridge Priority – 共通する内部のスパニング(CST)のブリッジプライオリティを指定します。値は 0 から 61440 までの間。 4096 の倍数に設定されます。たとえばプライオリティを 0 から 4095 の間にセットしようとすれば、それは 0 に設定されます。たとえば 4096 から(4096 -1)の間にセットしようとすれば 4096 に設定されます。 デフォルトプライオリティは 32768 です。

Bridge Max Age – 共通する内部のスパニングツリー(CST)の最大エイジを指定します。値は 6 から 40 で、その値は「2*(ブリッジ転送遅延時間 – 1) より小さいか同等で、「2*(ブリッジhelloタイム + 1)より大きいか同等とします。デフォルトは 20 です。

Bridge Hello Time – 共通する内部スパニングツリー(CST)のためのブリッジhelloタイムを指定します。値は「(ブリッジ最大エイジ/2) – 1」より小さいか同等とします。デフォルトは 2 です。

Bridge Forward Delay – パケットを転送する前に「リスニングとラーニング」モードで費やされる時間を指定します。ブリッジ転送遅延時間は「(ブリッジ最大エイジ/2) +1」より大きいか同等でなければならず、デフォルトは 15 です 。

Spanning Tree Maximum Hops – スパニングツリーの最大限ホップ数を構成します。

構成不可能なデータ

Bridge identifier – CSTのブリッジ識別子です。ブリッジのプライオリティとブリッジのベースのMAC ドレスから構成されます。

Time since topology change – CSTのトポロジーが最後に変更されてからの秒数。

Topology change count – CSTのためにトポロジーが変更された回数。

Topology change – CSTに割当てられたポートでトポロジー変更が進行中かどうかを表示する、トポロジー変更パラメータの値。

Designated root – ルートのブリッジのブリッジ識別子。ブリッジプライオリティとブリッジのベースMACアドレスから構成される。

Root Path Cost – CSTの指定されたルートへのパス・コスト値

Root Port – CSTの指定されたルートにアクセスするポート

Max Age – CSTの指定されたルートへのパス・コスト値

Forward Delay – ルートポートブリッジの転送遅延時間パラメータからの発生値

Hello Time - ルートポートブリッジのhelloタイムパラメータからの発生値

Hold Time – 構成BPDUを送信する間隔の最小時間。

CST Regional Root – CST局所ルートのプライオリティとベースMACアドレス。

CST Path Cost – CSTツリーの局所ルートへのパス・コスト値。

コマンドボタン

Apply - 新しい構成を適用し変更を有効化します。これらの変更は構成を保存しなければ電源を切ると保持されません。

Refresh - 最新データで更新します。

8.3.19.3 MST

						Spanning Tree
Switch Config/Status	CST	MST	CST Port	MST Port	Statistics	

MST: Create

MST ID (1 to 4094) :* 0

* = mandatory

Apply

図 ： スパニングツリーMST 構成

選択基準

MST ID – 構成する新しいMSTまたはすでに存在するMSTを構成します。

構成可能データ

MST ID – これはMST ID選択ボックスの選択オプションが選択されているときのみ見えます。 作成されるMSTのIDの有効な値は 1 から 4094 までの値です。

Priority – 選択されたMSTインスタンスのブリッジプライオリティ。 ブリッジプライオリティは 4096 の倍数で設 定されます。たとえばプライオリティを 0 から 4095 の間にセットしようとすれば 0 に設定されます。4096 から(2*4096 -1)にセットしようとしたら 4096 に設定されます。

VLAN ID – これはスイッチ上のすべてのVLANのリストを提供します。選択されているMSTインスタンスと関 連付けられたVLANはリストでハイライト表示されます。これらはVLANの関連付けをMSTインスタンスへ再構成するために選択されたり選択を解除されたりできます。

構成不可能なデータ

Bridge identifier – 選択されたMSTインスタンスのブリッジ識別子です。ブリッジのプライオリテ ィとブリッ ジのベースのMACドレスから構成される。

Time since topology change – 選択されたMSTインスタンスのトポロジーが最後に変更されてからの秒数。

Topology change count – 選択されたMSTインスタンスのためにトポロジーが変更された回数。

Topology change – 選択されたMSTインスタンスに割当てられたポートでトポロジー変更が進行 中かどうかを表示する、トポロジー変更パラメータの値。 真か偽かの値を取ります。

Designated root – ルートブリッジのブリッジ識別子。ブリッジプライオリティとブ リッジのベースMACア ドレスから成っています。

Root Path Cost – このMSTインスタンスのため指定されたルートへのパス･コスト値。

Root port – このMSTインスタンスのため指定されたルートへアクセスするポート。

コマンドボタン

Apply - 新しい構成を適用し変更を有効化します。これらの変更は構成を保存 しなければ電源を切 ると保持されません。

Delete - 選択したMSTインスタンスを削除します。このインスタンスに関連付けられ たすべての VLAN はCSTに関連付けられています。

Refresh - 最新データで更新します。

8.3.19.4 CST ポート

Spanning Tree

Switch Config/Status | CST | MST | CST Port | MST Port | Statistics

Slot/Port:	Encl-CB1/0/1
Port Priority (0 to 240) :*	128
Admin Edge Port :	Enable
Port Path Cost (0 to 200000000) 0 = Auto :*	0
Auto-calculate Port Path Cost:	Enabled
External Port Path Cost (0 to 200000000) 0 = Auto :*	0
Auto-calculate External Prt Path Cost:	Enabled
Port ID :	80:01
Port Up Time Since Counters Last Cleared:	0 day 3 hr 45 min 16 se
Port Mode:	Enable
Port Forwarding State :	Disabled
Port Role :	Disabled
Designated Root:	80:00:00:23:8b:17:7b:85
Designated Cost :	0
Designated Bridge :	80:00:00:23:8b:17:7b:85
Designated Port :	00:00
Topology Change Acknowledge :	False
Edge Port:	Disabled
Point-to-point MAC:	False
CST Regional Root:	80:00:00:23:8b:17:7b:85
CST Path Cost :	0

* = mandatory

Apply | Refresh | Force

図 ： スパニングツリーCST ポート構成

選択基準

Slot/Port – CSTに関連付けられたVLANと関連付けられた物理またはポートチャンネル のインターフェイスから 1 個を選択します。

Admin Edge Port - 指定したポートがCIST内のエッジポートであれば選択します。有効化か無 効化の値を取ります。デフォルトは無効化です。

Port Mode - ポートかポートチャンネルに関連付けられたスパニングツリープロ トコルの管理モードです。可能な値は有効化または無効化です。

構成可能データ

Port Priority – CST内の特定のポートのプライオリティです。ポートプライオリティは 16 の倍数に設定されます。 たとえばプライオリティを 0 から 15 の間の値にセットしようとすればそれは 0 になります。16 と(2*16 – 1) の間の値にセット使用すると 16 になります。

Port Path Cost – 共通する内部のスパニングツリーの特定のポートに新しい値のパス･コストを設定します。 1 から 200000000 の範囲の値を使います。

External Port Path Cost - スパニングツリーの特定のポートに新しい値の外部ポストのパス･コストを設 定します。 1 から 200000000 の範囲の値を取ります。

構成不可能なデータ

Auto-calculate Port Path Cost – パス･コストを自動で計算する(有効)かしないか(無効)を表示します。パ ス･コスト値はポートパス･コストがゼロに構成されている場合ポートのリンク速度に基づいてパス･コストが計算されます。

Auto-calculate External Port Path Cost – 外部パス・コストを自動で計算する(有効)かしないか(無効) を表示します。外部のパス・コスト値は外部ポートパス・コストがゼロに構成されている場合ポート のリンク速度に基づいてパス・コストが計算されます。

Port ID – CST内の特定されたポートのためのポート識別子です。ポートプライオリティとポートの インターフェイス数から作成されます。

Port Up Time Since Counters Last Cleared – カウンターが最後にクリアされて以降の時間 、日、時間、分、と秒とで表示されます。

Port Forwarding State – このポートの転送状態。

Port Role - 有効にされている各MSTブリッジポートは各スパニン グツリーに対しポートの 役割が割当てられます。

Designated Root - CSTのルートブリッジです。ブリッジプライオリティとブリッジの ベースMACアドレスから構成されます。

Designated Cost – 指定されたポートによりLANに提供されるパス・コスト値。

Designated Bridge – 指定されたポートのあるブリッジの識別子。 ブリッジプライオリティ とブリッジのベースMACアドレスから構成されます。

Designated Port – LANへ最小のコストを申し入れる指定されたブリッジにあるポート識別子。 ポートプライオリティとポートのインターフェイス数から構成されます。

Topology Change Acknowledge – このポートへ送信される次のBPDUがトポロジー 変更の通知フラッグセットを持つ かどうかを識別します。 値は真または偽です。

Edge port – ポートがエッジポートとして有効化されたかどうかを示します。「有効化」か「無効化」の値を取ります。

Point-to-point MAC – 点間状態の派生値。

CST Regional Root – CST局所ルートのためのブリッジ識別子。 ブリッジプライオリティとブリ ッジのベースMACアドレスから作成されます。

CST Path Costー CST局所ルートへのパス・コスト値

コマンドボタン

Apply - 新しい構成を適用し変更を有効化します。これらの変更は構成を保存しなければ電源を切ると保持されません。

Force – このボタンをクリックするとポートを強制して 802.1w または 802.1d BPDUを送信させます。

Refresh - 最新データで更新します。

8.3.19.5 MST ポート

Spanning Tree

Switch Config/Status | CST | MST | CST Port | MST Port | Statistics

MST ID :	1
Slot/Port:	Encl-CB1/0/1
Port Priority (0 to 240) :*	128
Port Path Cost (0 to 200000000) 0 = Auto :*	0
Auto-calculate Port Path Cost:	Enabled
Port ID :	80:01
Port Up Time Since Counters Last Cleared:	0 day 0 hr 0 min 2 sec
Port Mode:	Enabled
Port Forwarding State:	Disabled
Port Role:	Disabled
Designated Root:	80:01:00:23:8b:17:7b:85
Designated Cost:	0
Designated Bridge :	80:01:00:23:8b:17:7b:85
Designated Port :	00:00

* = mandatory

Apply Refresh

図 ： スパニングツリーMST ポート構成

選択基準

MST ID -既存MSTインスタンスから 1 つMSTインスタンスを選択します。

Slot/Port – 選択されたMSTインスタンスに関連付けられたVLANに関連付けられた 物理また はポートチャンネルのインターフェイスを 1 個選択します。

構成可能データ

Port Priority – 選択されたMSTインスタンス内の特定ポートのプライオリティです。ポートプライオ リティは 16 の倍数で設定されます。たとえば 0 から 15 の間の値をセットしようとすればゼロに設定されます。 16 と(2*16 -1)の間の値にセットしようとすれ 16 に設定されます。

Port Path Cost – 選択されたMSTインスタンスの中の特定のポートに新しい値でパス･コストを設定します。 1 から 200000000 の範囲の値を取ります。

構成不可能なデータ

Auto-calculate Port Path Cost – パス･コストを自動で計算する(有効)かしないか(無効)を表示します。パス･コスト値はポートパス･コストがゼロに構成されている場合ポートのリンク速度に基づいてパス･コストが計算されます。

Port ID – 選択されたMSTインスタンス内で指定されたポートのための識別子。ポストプライオリテ ィとポートのインターフェイス数から構成されます。

Port Up Time Since Counters Last Cleared – カウンターが最後にクリアされて以降の時 間、日、時間、分、と秒とで表示されます。

Port Mode – ポートまたはポートチャンネルに関連付けられたスパニングツリーの管 理モードです。 可能な値は有効化 または無効化です。

Port Forwarding State – このポートの転送状態。

Port Role - 有効にされている各MSTブリッジポートは各スパニングツリーに対しポートの役割が 割当てられます。

Designated Root - MSTのルートブリッジです。ブリッジプライオリティとブ リッジのベースMACアドレスから構成されます。

Designated Cost – 指定されたポートによりLANに提供されるパス・コスト値。

Designated Bridge – 指定されたポートのあるブリッジの識別子。 ブリッジプライオリティとブリッジのベースMACアドレスから構成されます。

Designated Port – LANへ最小のコストを申し入れる指定されたブリッジにあるポート識別子。 ポートプライオリティとポートのインターフェイス数から構成されます。

コマンドボタン

Apply - 新しい構成を適用し変更を有効化します。これらの変更は構成を保存しなければ電源を切ると保持されません。

Refresh - 最新データで更新します。

8.3.19.6　統計

図 : スパニングツリーMST ポート統計

選択基準

Slot/Port –　スイッチの物理またはポートチャンネルのインターフェイスのひとつを選択します。

構成不可能なデータ

STP BPDUs Received – 選択したポートで受信したSTP BPDUの数

STP BPDUs Transmitted – 選択したポートから送信したSTP BPDUの数

RSTP BPDUs Received – 選択したポートで受信したRSTP BPDUの数

RSTP BPDUs Transmitted – 選択したポートから送信したRSTP BPDUの数

MSTP BPDUs Received – 選択したポートで受信したMSTP BPDUの数

MSTP BPDUs Transmitted – 選択したポートから送信したMSTP BPDUの数

コマンドボタン

Refresh -　最新データで更新します。

8.3.20 リンク･ステート

8.3.20.1 構成

Link State

Config | Status

Admin Mode: Disable
Group ID: Create New Group
Group Mode: Disable
Up stream Port:
Down stream Port: Encl-CB1/0/1 Encl-CB1/0/2 Encl-CB1/0/3 Encl-CB1/0/4 Encl-CB1/0/5

Apply

図 ： リンク･ステート 構成

選択基準

Admin Mode－ プルダウンメニューから有効化または無効化を選択しスイッチのリンク･ステート管理モードを選びます。

Group ID — 既存グループを再構成するか新規作成にこの画面を使用します。

Group Mode — プルダウンメニューから有効化または無効化を選択しスイッチのグループ管理モードを選びます。

Upstream — グループのアップストリームポートを選びます。スイッチは冗長LANポートを高速にフェイルオーバーするためリンクレベルを監視します 。

構成可能データ

ダウンストリーム – グループのダウンストリームポートを選ぶ。スイッチはこれらダウンストリームポートをアップストリームポートに関連付けます。アップストリームポートのリンクに障害があると、すべてのダウンストリームは無効化されます。それ以外の場合、有効化されています。

コマンドボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても新しい設定をスイッチに保持させるには保存しなければなりません

Delete - このグループを削除する。

8.3.20.2　**ステータス**

このページはすべての構成されたリンク･ステートのステータスを表示します。

Port Channel	Port Channel Name	Port Channel Type	Admin Mode	Static Capability Mode	Link State	STP Mode	Link Trap	Configured Ports	Active Ports	Load Balance

図：リンク･ステートのステータス

構成不可能なデータ

Admin Modeーリンク･ステート機能の管理モード。

Group IDーリンク･ステートのグループID。グループIDの範囲は1～6です。

Modeーグループの管理モード。

Upstream portー 監視されているアップリンクポートおよびこのアップリンクポイントのリンク･ステート。

Downstream portsーリンク･ステートのダウンリンクポート。

コマンドボタン

Refresh -　スイッチの現在のデータ状態で画面のデータを更新します。

8.3.21 ポートのバックアップ

8.3.21.1 構成

2個のポートは 1 個のグループに関連付けられています。2個のポートはアクティブとバックアップポートとして動作します。2個のポートのうち 1 回に 1個ずつアクティブになります。構成されたアクティブポートはリンクアップなので、バックアップポートは無効化されます。それ以外の場合、アクティブなポートがリンクダウンなら、構成されたバックアップポートは有効化されます。グループの 2 個のポートはグループが有効化される前にすべてリンクアップとなり、構成されたアクティブは「アクティブ」になるよりも高いプライオリティを持ちます。

Port-backup

Config | Status

Admin Mode: Disabled
Group ID: Create
Group Mode: Disabled
Active Port:
Backup Port:

Apply | Delete

図 : ポートのバックアップ 構成

選択基準

Admin Mode – 有効化か無効化を選択してスイッチのポートバックアップの管理モードを選ぶ。工場側デフォルトは無効化されている。

Group ID – グループID – この画面により既存グループを再構成するか新しいグループを作成します。このプルダウンメニューにより既存グループから 1 個を選ぶか「作成」を選んで新規グループを追加します。

Group Mode – プルダウンメニューから有効化または無効化を選んでスイッチのグループ管理モードを選びます。工場側デフォルトは無効化されているこのグループをアクティブポートとして有効化しバックアップポートが構成されます。

Active port – 1 個のグループ用にアクティブポートを構成します。6 個の 1Gbpsへの 6 組のポートはアクティブに構成できます。

Backup port – 1 個のグループ用にバックアップポートを選びます。6 個の 1 Gbps用の 6 組のポートはバックアップポートに構成できます。

コマンドボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても、新しい設定をスイッチ に保持させるには保存しなければなりません

Delete - このグループを削除する。

8.3.21.2 **ステータス**

このページは構成されたポートバックアップの現状を表示します。

Port-backup

Config | Status

Admin Mode : Disable

Group ID	Mode	Active Port	Backup Port	Current Active Port

Refresh

図 : ポートバックアップのステータス

構成不可能なデータ

Admin Mode－　ポート･バックアップ機能の管理モード。

Group ID – ポートバックアップのグループのID。グループID の範囲は 1 から 6 です。

Mode – このグループの管理モード。

Active port – このグループの構成されたアクティブポート。

Backup port – このグループの構成されたバックアップポート。

Current Active port – このグループの現在アクティブポート。

コマンドボタン

Refresh -　スイッチの現在のデータ状態で画面のデータを更新します。

8.3.22 MACフィルター

8.3.22.1 構成

図：MAC フィルター構成

選択基準

MACフィルター ― これはすべての構成されたフィルターのためのMACアドレスとVLAN IDの組み合わせのリストです。既存フィルターのポートマスクを変更するには変更するエントリを選択します。 新しいフィルターを追加するには「Create Filter」をリストのトップから選択します 。

VLAN ID – フィルターするパケットを完全に識別するためのVLAN IDとMACアドレスです。「Create Filter」オプションを選んだ場合のみこの欄は変更できます 。

構成可能データ

MAC アドレス - 00:01:1A:B2:53:4D形式によるフィルターのMACアドレス。「Create Filter」オプションを選んでいたときはこの欄を変更できるだけです。 これらのMACアドレスのためにフィルターは定義できません 。

- 00:00:00:00:00:00
- 01:80:C2:00:00:00 to 01:80:C2:00:00:0F
- 01:80:C2:00:00:20 to 01:80:C2:00:00:21
- FF:FF:FF:FF:FF:FF
- 01:00:5E:00:00:00 to 01:00:5E:FF:FF:FF
- 33:33:00:00:00:00 to 33:33:FF:FF:FF:FF

ソース・ポート・メンバー – 受信側のフィルターに含むポートをリストします。選択したMACアドレスとVLAN IDのあるパケットがリストにないポートで受信されると破棄されます。

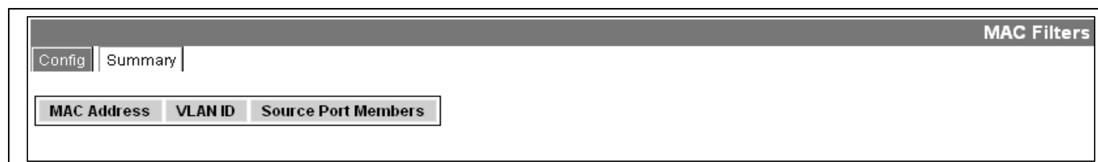
コマンドボタン

Apply - 画面の設定でスイッチを更新する。パワーサイクル後、新しい設定をスイッチに保持させるには保存しなければなりません 。

Delete - 現在選択されたフィルターを削除します。

Delete All – 構成されたすべてのフィルターを削除します。

8.3.22.2 **サマリー**



図：MAC フィルター　サマリー

構成不可能なデータ

MAC Address - 00:01:1A:B2:53:4D 形式によるフィルターのMACアドレスです。

VLAN　ID – フィルターに関連付けられたVLAN ID。

Source Port Members – 受信されたパケットをフィルタリングするために使われるポートのリスト。

8.4 セキュリティ･メニュー

8.4.1 ポートアクセス制御

8.4.1.1 構成

Port Access Control

Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary

Administrative Mode: Disable

Apply

図 : :ポートアクセス制御の構成

選択基準

Administrative Mode - このセレクタは管理モードの 2 つのオプションをリストする: 有効化と無効化である。 デフォルト値は無効化である。

コマンドボタン

Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければパワーサイクルでは保持されません 。

8.4.1.2 ポート･コンフィグ

Port Access Control

Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary

Port :	Encl-CB1/0/1
Control Mode:	Auto
Quiet Period (secs) (0 to 65535) :*	60
Transmit Period (secs) (1 to 65535) :*	30
Supplicant Timeout (secs) (1 to 65535) :*	30
Server Timeout (secs) (1 to 65535) :*	30
Maximum Requests (1 to 10) :*	2
Reauthentication Period (secs) (1 to 65535) :*	3600
Reauthentication Enabled:	False

* = mandatory

Initialize | Reauthenticate | Apply | Refresh

図 ： ポート･アクセス制御ポート･コンフィグ

選択基準

Port - 構成すべきポートを選択する。 この選択が変更されると、画面が更新されてすべての欄は新たに選択されたポートに更新される。 すべての物理インターフェイスは有効である。

Control Mode - このセレクタは制御モードのオプションをリストする。 制御モードはポートのリンク･ステータスがリンクアップである場合のみ設定される。 オプション：

- 非認証強制: 認証コード･ポート･アクセス･エンティティ (PAE)は制御されるポートを無条件に非認証に設定する。
- 認証強制: 認証コード･ポート･アクセス･エンティティ (PAE)は制御されるポートを無条件に認証に設定する。
- auto: 認証コードPAEはポート･モードを認証請求者、認証コード、および認証サーバの間の認証交換結果を反映するうに設定する。

Reauthentication Enabled - この選択欄から指定されたポートの認証請求者を再認証するかを有効化または無効化できる。 選択可能な値は'true'/真と'false'/偽である。 再認証はこの値が'true'/真のときに行われる。 真でなければ再認証は許可されない。 デフォルト値は'false'/偽である。 この選択を変えてもApplyボタンを押すまでは構成は反映しない 。

構成可能データ

Quiet Period - この選択欄から選択されたポートに不感時間を構成できる。 このコマンドはこのポートで認証コードステート･マシンが使用するタイマーの秒単位の値を認証請求者を取得しようとしない時間に設定する。 不感時間とは、認証請求者との認証交換の失敗後、認証コード認証請求者を取得しようとしない時間である。 不感時間は 0 と 65535 の間の数字とする。不感時間が 0 とは認証コードステート･マシンは認証請求者を取得することはないことを意味する。 デフォルト値は 60 である。この値を変化させてもApplyボタンを押すまでは構成を変更しない。

Transmit Period - この入力欄から選択されたポートに送信時間を構成できる。 送信時間は、認証請求者にEAPOL EAP要求/アイデンティティ･フレームをいつ送るかを決めるための、指定されたポートで認証コードステート･マシンが使用するタイマーの秒単位の値である。 送信時間は 1 から 65535 の範囲の数字とする。デフォルト値は 30 である。この値を変化させてもApplyボタンを押すまでは構成を変更しない。

Supplicant Timeout - この入力欄から選択されたポートに認証請求者タイムアウトを入力できる。 この認証請求者タイムアウトは認証請求者をタイムアウトするまでの、指定されたポートで認証コードステート・マシンが使用するタイマーの秒単位の値である。 認証請求者タイムアウトは 1 から 65535 の範囲の数字とする。デフォルト値は 30 である。 この値を変化させてもApplyボタンを押すまでは構成を変更しない。

Server Timeout - この入力欄から選択されたポートにサーバ・タイムアウトを入力できる。 サーバ・タイムアウトは認証サーバをタイムアウトするまでの、指定されたポートで認証コードが使用するタイマーの秒単位の値である。 サーバ・タイムアウトは 1 から 65535 の範囲の数字とする。デフォルト値は 30 である。 この値を変化させてもApplyボタンを押すまでは構成を変更しない。

Maximum Requests - この入力欄から選択されたポートに最大要求回数を入力できる。 最大要求回数値は認証請求者をタイムアウトするまでのEAPOL EAP要求/アイデンティティをこのポートで認証コードステート・マシンが再送する最大回数である。 最大要求回数は 1 から 10 の範囲の数字とする。デフォルト値は 2 である。 この値を変化させてもApplyボタンを押すまでは構成を変更しない。

Reauthentication Period - この入力欄から選択されたポートに再認証時間を入力できる。 再認証時間は認証請求者の再認証が行われる時を定める、指定されたポートで認証コードステート・マシンが使用するタイマーの秒単位の値である。 再認証時間は 1 から 65535 の範囲の数字とする。デフォルト値は 3600 である。この値を変化させてもApplyボタンを押すまでは構成を変更しない。

コマンド・ボタン

Initialize - このボタンは選択されたポートで初期化シーケンスを開始する。 このボタンは制御モードが'auto'である場合のみ選択できる。 このボタンが選択不可の場合はグレイアウトされ何もできない。 このボタンを押すと、動作は直ちに適用される。 この動作が生じるにはApplyボタンを押す必要がない。

Reauthenticate - このボタンは選択されたポートで再認証シーケンスを開始する。 このボタンは制御モードが'auto'である場合のみ選択できる。 このボタンが選択不可の場合はグレイアウトされ何もできない。 このボタンを押すと、動作は直ちに適用される。 この動作が生じるにはApplyボタンを押す必要がない。

Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければパワーサイクルでは保持されません 。

Refresh - デフォルト値は 3600 である。

8.4.1.3 ポートステータス

Port:	Encl-CB1/0/1
Control Mode:	Auto
Quiet Period (secs):	60
Transmit Period (secs):	30
Supplicant Timeout (secs):	30
Server Timeout (secs):	30
Maximum Requests :	2
Reauthentication Period (secs):	3600
Reauthentication Enabled:	False
Control Direction:	Both
Protocol Version:	1
PAE Capabilities:	Authenticator
Authenticator PAE State:	Initialize
Backend State:	Initialize

Port Access Control

Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary

Refresh

図 ： ポート･アクセス制御ポート･ステータス

選択基準

Port -表示すべきポートを選択する。 この選択が変更されると、画面が更新されてすべての欄は新たに選択されたポートに更新される。 すべての物理インターフェイスは有効である。

構成不可能なデータ

Control Mode: 指定されたポートに構成された制御モードを表示する。 オプション:

- 非認証強制:
- 認証コード･ポート･アクセス･エンティティ (PAE)は制御されるポートを無条件に非認証に設定する
- 認証強制: 認証コード･ポート･アクセス･エンティティ (PAE)は制御されるポートを無条件に認証に設定する。
- auto:認証コードPAEはポート･モードを認証請求者、認証コード、および認証サーバの間の認証交換結果を反映するうに設定する。

Quiet Period -このフィールドは選択されたポートに構成された不感時間を表示する。 この不感時間は認証請求者を取得しようとしない時間を定めるこのポートで認証コードステート･マシンが使用するタイマーの秒単位の値である。 不感時間とは、認証請求者との認証交換の失敗後、認証コード認証請求者を取得しようとしない時間である。 不感時間は 0 から 65535 の範囲の数字である。

Transmit Period -このフィールドは選択されたポートに構成された送信時間を表示する。 送信時間は、認証請求者にEAPOL EAP要求/アイデンティティ･フレームをいつ送るかを決めるための、指定されたポートで認証コードステート･マシンが使用するタイマーの秒単位の値である。 送信時間は 1 から 65535 の範囲の数字である。

Supplicant Timeout -このフィールドは選択されたポートに構成された認証請求者タイムアウトを表示する。 この認証請求者タイムアウトは認証請求者をタイムアウトするまでの、指定されたポートで認証コードステート･マシンが使用するタイマーの秒単位の値である。 認証請求者タイムアウトは 1 から 65535 の範囲の数字である。

Server Timeout -このフィールドは選択されたポートに構成されたサーバ･ムアウトを表示する。 サーバ･タイムアウトは認証サーバをタイムアウトするまでの、指定されたポートで認証コードが使用するタイマーの秒単位の値である。 認証請求者タイムアウトは 1 から 65535 の範囲の数字である。

Maximum Requests - この欄は選択されたポートへの構成された最大要求回数を表示する。 最大要求回数値は

認証請求者をタイムアウトするまでのEAPOL EAP要求/アイデンティティをこのポートで認証コードステート・マシンが再送する最大回数である。 最大要求回数は 1 から 10 までの値である。

Reauthentication Period - この欄は選択されたポートに構成された再認証時間を表示する。 再認証時間は認証請求者の再認証が行われる時を定める、指定されたポートで認証コードステート・マシンが使用するタイマーの秒単位の値である。 認証請求者タイムアウトは 1 から 65535 の範囲の数字である。

Reauthentication Enabled - この欄は選択されたポートに再認証が有効化されているかを表示する。 この欄は構成できる。 可能な値は'true'/真と'false'/偽である。 再認証はこの値が'true'/真のときに行われる。 真でなければ再認証は許可されない。

Control Direction - 指定されたポートでの制御方向を表示する。 制御方向は認証請求者と認証コードの間で行われるプロトコル交信のレベルを決定する。 これは未認証の被制御ポートが両方向通信(入出フレームを両方とも無効化) またはインバウンドのみか(インバウンド・フレームの受信を無効化)を制御するかに影響する。 この欄は一部のプラットフォームでは構成できない。

Protocol Version - この欄は選択されたポートに関連付けられたプロトコル・バージョンを表示する。 1のみ可能な値であり、これは 802.1x規格の最初のバージョンに対応する。 この欄は構成できない。

PAE Capabilities - この欄は選択されたポートのポート・アクセス・エンティティ(PAE)の機能を表示する。 とりえる値は"Authenticator"(認証コード)または"Supplicant"(認証請求者) である。 この欄は構成できない。

Authenticator PAE State - この欄は認証コードPAEのステート・マシンの現状を表示する。 とりうる値:

- "Initialize" (初期化)
- "Disconnected" (非接続)
- "Connecting"(接続中)
- "Authenticating"(認証中)
- "Authenticated"(認証完了)
- "Aborting"(中止中)
- "Held"(一時停止中)
- "ForceAuthorized"(強制認証)
- "ForceUnauthorized"(強制非認証)

Backend Authentication State - この欄はバックエンド認証ステート・マシンの現状を表示する。 とりうる値:

- "Request"(要求)
- "Response"(応答)
- "Success"(成功)
- "Fail"(失敗)
- "Timeout"(タイムアウト)
- "Initialize" (初期化)
- "Idle"(アイドル)

コマンド・ボタン

Refresh - デフォルト値は 3600 である。

8.4.1.4 ポート･サマリ

Port Access Control

Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary

Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Port Status
Encl-CB1/0/1	Auto	Auto	False	Authorized
Encl-CB1/0/2	Auto	Auto	False	Authorized
Encl-CB1/0/3	Auto	Auto	False	Authorized
Encl-CB1/0/4	Auto	Auto	False	Authorized
Encl-CB1/0/5	Auto	Auto	False	Authorized
Encl-CB1/0/6	Auto	Auto	False	Authorized
Encl-CB1/0/7	Auto	Auto	False	Authorized
Encl-CB1/0/8	Auto	Auto	False	Authorized
Encl-CB1/0/9	Auto	Auto	False	Authorized
Encl-CB1/0/10	Auto	Auto	False	Authorized
Encl-CB1/0/11	Auto	Auto	False	Authorized
Encl-CB1/0/12	Auto	Auto	False	Authorized
Encl-CB1/0/13	Auto	Auto	False	Authorized
Encl-CB1/0/14	Auto	Auto	False	Authorized
Encl-CB1/0/15	Auto	Auto	False	Authorized
Encl-CB1/0/16	Auto	Auto	False	Authorized
Encl-CB1/0/17	Auto	Auto	False	Authorized
Encl-CB1/0/18	Auto	Auto	False	Authorized
Encl-CB1/0/19	Auto	Auto	False	Authorized
Encl-CB1/0/20	Auto	Auto	False	Authorized
Encl-CB1/0/21	Auto	Auto	False	Authorized
Encl-CB1/0/22	Auto	Auto	False	Authorized
Encl-CB1/0/23	Auto	Auto	False	Authorized
Encl-CB1/0/24	Auto	Auto	False	Authorized
Encl-CB1/0/25	Auto	Auto	False	Authorized
Encl-CB1/0/26	Auto	Auto	False	Authorized

図 ： ポート･アクセス制御ポート･サマリ

構成不可能なデータ

Port -現在のテーブル行に設定が表示されるポートを指定する。

Control Mode - この欄はポートの構成された制御モードを示す。 とりうる値：

- 非認証強制: 認証コード･ポート･アクセス･エンティティ (PAE)は制御されるポートを無条件に非認証に設定する
- 認証強制: 認証コード･ポート･アクセス･エンティティ (PAE)は制御されるポートを無条件に認証に設定する。
- Auto: 認証コードPAEはポート･モードを認証請求者、認証コード、および認証サーバの間の認証交換結果を反映するうに設定する。

Operating Control Mode - この欄はポートが現在動作中の制御モードを示す。 とりうる値：

- "ForceUnauthorized"(強制非認証)
- "ForceAuthorized"(強制認証)
- Auto
- N/A： ポートが外された状態にあるとポート･アクセス制御には参加できない。

Reauthentication Enabled - この欄は指定されたポートの認証請求者の再認証が許可されているかを示す。 可能な値は'true'/真と'false'/偽である。 再認証はこの値が'true'/真のときに行われる。 真でなければ再認証は許可されない。 .

Port Status - この欄は指定されたポートの認証状態を示す。 とりうる値は'Authorized'(認証された),

'Unauthorized'(拒否された)および'N/A'(不明)である。 ポートが外された状態にあると、ポートはポート･アクセス制御に参加できないのでこの値は'N/A'になる。

コマンド･ボタン

Refresh - ページ情報を更新する。

8.4.1.5 統計

Port Access Control

Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary

Port :	Encl-CB1/0/1
EAPOL Frames Received:	0
EAPOL Frames Transmitted:	0
EAPOL Start Frames Received:	0
EAPOL Logoff Frames Received:	0
Last EAPOL Frame Version:	0
Last EAPOL Frame Source:	00:00:00:00:00:00
EAP Response/ID Frames Received:	0
EAP Response Frames Received:	0
EAP Request/ID Frames Transmitted:	0
EAP Request Frames Transmitted:	0
Invalid EAPOL Frames Received:	0
EAPOL Length Error Frames Received:	0

Refresh | Clear All | Clear

図 : ポート･アクセス制御統計

選択基準

Port - 表示すべきポートを選択する。この選択が変更されると、画面が更新されてすべての欄は新たに選択されたポートに更新される。 すべての物理インターフェイスは有効である。

構成不可能なデータ

EAPOL Frames Received- 認証コードが受信した有効な任意のタイプのEAPOLフレーム数を表示する。

EAPOL Frames Transmitted- 認証コードが送信した有効な任意のタイプのEAPOLフレーム数を表示する。

EAPOL Start Frames Received- 認証コードが受信した有効な任意のタイプのEAPOL開始フレーム数を表示する。

EAPOL Logoff Frames Received- 認証コードが受信した有効な任意のタイプのEAPOLログオフ･フレーム数を表示する。

Last EAPOL Frame Version- 直前に受信されたEAPOLフレームに運ばれたプロトコル･バージョン番号を表示する。

Last EAPOL Frame Source- 直前に受信されたEAPOLフレームに運ばれたソースMACアドレスを表示する。

EAPOL Response/Id Frames Received- 認証コードが受信したEAP応答/IDフレーム数を表示する。

EAP Response Frames Received- 認証コードが受信した有効なEAP応答フレーム数(応答/IDフレーム以外)を表示する。

EAP Request/Id Frames Transmitted- 認証コードが送信したEAP応答/IDフレーム数を表示する。

EAP Request Frames Transmitted- 認証コードが送信したEAP要求フレーム数(応答/IDフレーム以外)を表示す

る。

Invalid EAPOL Frames Received- フレーム･タイプが認識されずに認証コードが受信したEAPOLフレーム数を表示する。

EAP Length Error Frames Received- フレーム･タイプが認識されずに認証コードが受信したEAPOLフレーム数を表示する。

コマンド･ボタン

Refresh - デフォルト値は 3600 である。

Clear All -このボタンはすべてのポートのすべての統計を 0 にリセットする。確認プロンプトは表示されない。 このボタンが押されると、統計は直ちに消去される。

Clear -このボタンは選択されたポートの統計をリセットする。 確認プロンプトは表示されない。 このボタンが押されると、統計は直ちに消去される。

8.4.1.6 **ログイン**

Port Access Control
Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary
Users : Non-configured user
defaultList
Login:
Apply Refresh

図 ： ポート･アクセス制御ログイン

選択基準

Users - 802.1xポート･セキュリティに詮索されたログイン･リストを使用するユーザー名を選択する。

構成可能データ

Login - 指定されたユーザーに適用されるログインを選択する。 すべての構成されたログインが表示される 。

コマンド･ボタン

Apply - 更新した画面をスイッチへ送ります。 変更はスイッチ上で有効化されますが保存しなければこれらの変更は電源を切ると保持されません。

Refresh - デフォルト値は 3600 である。

8.4.1.7 **アクセス特権**

Port Access Control
Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary
Port : Encl-CB1/0/1
admin
guest
Users :
Apply Refresh

図 ： ポート･アクセス制御アクセス特権

選択基準

Port -構成するポートを選択する。

構成可能データ

Users - 指定されたポートにアクセスできるユーザーを選択する。

コマンド・ボタン

Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければパワーサイクルでは保持されません 。

Refresh - デフォルト値は 3600 である。

8.4.1.8 アクセス・サマリ

Port Access Control

Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary

Port	Users
Encl-CB1/0/1	admin guest
Encl-CB1/0/2	admin guest
Encl-CB1/0/3	admin guest
Encl-CB1/0/4	admin guest
Encl-CB1/0/5	admin guest
Encl-CB1/0/6	admin guest
Encl-CB1/0/7	admin guest
Encl-CB1/0/8	admin guest
Encl-CB1/0/9	admin guest
Encl-CB1/0/10	admin guest
Encl-CB1/0/11	admin guest
Encl-CB1/0/12	admin guest
Encl-CB1/0/13	admin guest
Encl-CB1/0/14	admin guest
Encl-CB1/0/15	admin guest
Encl-CB1/0/16	admin guest

図 : ポート・アクセス制御アクセス・サマリ

構成不可能なデータ

Port -ポートをスロット/ポート形式で表示する。

Users - ポートにアクセスできるユーザーを表示する。

コマンド・ボタン

Refresh - デフォルト値は 3600 である。

8.4.2 ポート･セキュリティ

8.4.2.1 構成

Port Security

Config | Interface Config | Static MAC Addresses | Dynamic MAC Addresses | Violation Status

Port Security Mode: Disable

Apply

図 ： ポート･セキュリティ･コンフィグ

構成可能データ

Port Security Mode- ポート･セキュリティ機能を有効化または無効化する。

コマンド･ボタン

Apply - 新構成を適用し変更は直ちに効力を発する。 当該変更は保存を実行しないとパワー･サイクル後、保持されない 。

8.4.2.2 インターフェイス･コンフィグ

Port Security

Config | Interface Config | Static MAC Addresses | Dynamic MAC Addresses | Violation Status

Slot/Port:	Encl-CB1/0/1
Port Security:	Disable
Maximum Number of Dynamically Learned MAC Addresses Allowed (0-600) :*	600
Add a Static MAC Address:	
VLAN ID (1-3965) :*	1
Maximum Number of Statically Locked MAC Addresses Allowed (0-20) :*	20
Enable Violation Traps:	No
Enable Violation Shutdown:	Disable
Clear Dynamically Learned MAC Addresses:	Clear
Convert dynamically locked address to statically locked:	Move

* = mandatory

Apply

図 ： ポート･セキュリティ･インターフェイス･コンフィグ

選択基準

Slot/Port - 構成すべきポートを選択する。

Port Security Mode - 選択されたインターフェイスにポート･セキュリティ機能を有効化または無効化する。

Enable violation traps - 許可されていないMACアドレスがあるパケットがロックされたポートで受信された際、新たなバイオレーショントラップ指定の送信を有効化または無効化する 。

Enable Violation Shutdown - 選択されたインターフェイスにポート･セキュリティバイオレーションシャットダウン･モードを有効化または無効化する 。

構成可能データ

Maximum Number of Dynamically Learned MAC Addresses Allowed - 選択されたインターフェイスで動的学習MACアドレスの最大数を設定する。

Add a static MAC address- 選択されたインターフェイスについてMACアドレスを静的にロックされたMACアドレス・リストに追加する。

VLAN ID - 選択されたインターフェイスについて静的にロックされたMACアドレス・リストに追加されるMACアドレスに対応するVLAN IDを追加する。

Maximum Number of Statically Learned MAC Addresses Allowed - 選択されたインターフェイスで静的にロックされたMACアドレスの最大数を設定する。

コマンド・ボタン

Clear - 選択されたインターフェイスの動的MACアドレスを消去する。

Move - 動的学習MACアドレスを静的にロックされたアドレスに変換する。 動的MACアドレス・エントリは静的限界に到達するまで番号の昇順で静的MACアドレス・エントリに変換される。

Apply - 新構成を適用し変更はすぐに反映される。 変更は保存を実行しないとパワー・サイクル後、保持されない 。

8.4.2.3 静的MACアドレス

Port Security

Config | Interface Config | Static MAC Addreses | Dynamic MAC Addresses | Violation Status

Slot/Port: Encl-CB1/0/1

MAC Address | VLAN ID

Delete a static MAC Address:

VLAN ID (1-3965) : Apply

図 : ポート･セキュリティ静的 MAC アドレス

選択基準

Slot/Port - データを表示させる物理インターフェイスを選択する。

構成可能データ

MAC Address - 削除するMACアドレスのユーザー入力を受け入れる。

VLAN ID - 削除するMACアドレスに対応するVLAN IDのユーザー入力を受け入れる。

構成不可能なデータ

MAC Address - ユーザー定義の静的にロックされたMACアドレスを表示する。

VLAN ID - MACアドレスに対応するVLAN IDを表示する。

コマンド･ボタン

Apply - 新構成を適用し変更は直ちに効力を発する。 当該変更は保存を実行しないとパワー･サイクル後、保持されない。

8.4.2.4 動的MACアドレス

Port Security

Config | Interface Config | Static MAC Addreses | Dynamic MAC Addresses | Violation Status

Slot/Port: Encl-CB1/0/1

MAC Address | VLAN ID

図 : ポート･セキュリティ動的 MAC アドレス

選択基準

Slot/Port - データを表示させる物理インターフェイスを選択する。

構成不可能なデータ

MAC Address -特定のポートで学習されたMACアドレスを表示する。

VLAN ID - MACアドレスに対応するVLAN IDを表示する。

Number of Dynamic MAC addresses learned - 特定のポートで動的に学習されたMACアドレスの数を表示する。

8.4.2.5 バイオレーションステータス

Port Security

Config | Interface Config | Static MAC Addreses | Dynamic MAC Addresses | Violation Status

Slot/Port: Encl-CB1/0/1

Last Violation MAC address	VLAN ID

図 : ポート･セキュリティ動的違反ステータス

選択基準

Slot/Port - データを表示させる物理インターフェイスを選択する。

構成不可能なデータ

Last Violation MAC Address - ロックされたポートで破棄された直前のパケットのソースMACアドレスを表示する。

VLAN ID - 直前のバイオレーションMACアドレスに対応するVLAN IDを表示する 。

8.4.3 RADIUSを構成する

8.4.3.1 構成

Configuration

Config | Server Config | Accounting Server Config

Current Server:
Number of Configured Servers: 0
Max Number of Retransmits (1 to 15):* 4
Timeout Duration (secs) (1 to 30):* 5
Dead Time (secs) (1 to 255):* 255
Accounting Mode: Disable
Radius Attribute 4 (NAS-IP Address): 0 . 0 . 0 . 0

* = mandatory

Apply Refresh

図：RADIUS コンフィグ

選択基準

Accounting Mode - Selects if the RADIUSアカウンティング･モードの有効化または無効化を選択する。

構成可能データ

Max Number of Retransmits - 要求パケットが再送信される最大の回数の値。 この値の範囲は 1 から 15 までである。RADIUS最大送信数とRADIUSタイムアウトを構成する際は最大遅延時間を検討すること。 複数のRADIUSサーバを構成する場合、各サーバの最大再送信数は次のサーバが試行される前に消化される。 再送信は、RADIUSサーバから応答が無く当該サーバに構成されたタイムアウト値が経過するまでは、行われない。 従って、RADIUSアプリケーションからの応答を受信する最大遅延時間はすべての構成されたサーバの(再送信時間タイムアウト)合計に等しい。 RADIUS要求がユーザーのログイン試行により生成された場合、すべてのユーザー･インターフェイスはRADIUSアプリケーションが応答を返すまでブロックされる。

Timeout Duration (secs) - 要求再送信の秒単位によるタイムアウト値。この値の範囲は 1 から 30 までである。RADIUS最大送信数とRADIUSタイムアウトを構成する際は最大遅延時間を検討すること。 複数のRADIUSサーバを構成する場合、各サーバの最大再送信数は次のサーバが試行される前に消化される。 再送信は、RADIUSサーバから応答が無く当該サーバに構成されたタイムアウト値が経過するまでは、行われない。 従って、RADIUSアプリケーションからの応答を受信する最大遅延時間はすべての構成されたサーバの(再送信時間タイムアウト)合計に等しい。 RADIUS要求がユーザーのログイン試行により生成された場合、すべてのユーザー･インターフェイスはRADIUSアプリケーションが応答を返すまでブロックされる。

静止時間 – 秒単位の静止時間。 有効な範囲は 1 から 255 までである 。

Radius Attribute 4 (NAS-IP Address) - Radius要求にRadius属性 4 (NAS-IPアドレス)を含めることの有効化か無効化を選択する。 NAS-IPアドレスとしてRADIUSサーバに送られるIPアドレスを明示的に指定する。 指定されない場合、RADIUSサーバにパケットを送るために使用されるアウトバウンド･インターフェイスのIPアドレスがNAS-IPアドレスとして追加される。

構成不可能なデータ

Current Server - 現在のサーバのIPアドレスまたはホスト名。 この欄は構成されたサーバが無い場合は空白である。

Number of Configured Servers - 構成されたRADIUSサーバの数。 このは 0 から 3 の範囲とすること。

コマンド･ボタン

Apply - 更新した画面をスイッチへ送ります。 変更はスイッチ上で有効化されますが保存しなければこれらの変更は電源を切ると保持されません。

Refresh - デフォルト値は 3600 である。

8.4.3.2 サーバ･コンフィグ

図：RADIUS サーバ･コンフィグ

選択基準

RADIUS Server - 構成するRADIUS サーバを選択する。 サーバを追加するにはaddを選ぶ。

Primary Server - 選択されたサーバをプライマリまたはセカンダリ･サーバに設定する。

Message Authenticator - 選択されたサーバのメッセージ認証コード属性を有効化または無効化する。

構成可能データ

IP Address - 追加されたサーバのIPアドレス。
次のIPアドレスを使うことはできない:

- 0.0.0.0
- 255.255.255.255
- 224.xxx.xxx.xxx
- 127.0.0.1

Host Name - 追加されたサーバのホスト名

Port - このサーバが使用するUDPポート。 有効な範囲は 0 から 65535 までである。

Secret - このサーバに共有されるシークレット。 この欄は入力のみである。

Apply - シークレットはこのボックスがチェックオンされている場合のみ適用される。 このボックスがチェックオンされていない場合、シークレット欄に何を入力しても効果は無く保持されない。 この欄はユーザーがRead･Write特権を持つ場合のみ表示される。

Encrypted - シークレット文字列が暗号化される際はこのボックスがチェックオンされていること。 この欄はユーザーがRead･Write特権を持つ場合のみ表示される。

構成不可能なデータ

Current - このサーバが現在認証サーバとして使用中であることを示す。

Secret Configured - このサーバの共有シークレットが構成されたことを示す。

コマンド・ボタン

Apply –更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければパワーサイクルでは保持されません

。

Remove - 選択されたサーバを構成から削除する。 このボタンはRead・Write特権ユーザーにのみ利用できる。変更は保存を実行しなければパワー・サイクル後、保持されない

。.

Refresh - デフォルト値は 3600 である。

8.4.3.3 アカウンティング･サーバ･コンフィグ

Configuration				
Config	Server Config	Accounting Server Config		
Accounting Server:	Add			
IP Address	.	.	.	
* = mandatory				
		Apply		

図：RADIUS アカウンティング･サーバ･コンフィグ

選択基準

Accounting Server - データが表示されるまたは構成されるアカウンティング･サーバを選択する。 add item/項目を追加するが選択されると、新たなアカウンティング･サーバを構成できる。

構成可能データ

IP Address: 追加するアカウンティング･サーバのIPアドレス。Add項目が選択されているときのみこの欄は構成できる 。
次のIPアドレスを使うことはできない:

- 0.0.0.0
- 255.255.255.255
- 224.xxx.xxx.xxx
- 127.0.0.1

Host Name - 追加されたサーバのホスト名

Port -アカウンティング･サーバが使用するUDPポートを指定する。 有効な範囲は 0 から 65535 までである。Read Only特権ユーザーには値は表示されるが変更はできない。

Secret- 指定されたアカウンティング･サーバと使用する共有シークレットを指定する。 この欄はユーザーがRead･Write特権を持つ場合のみ表示される。

Apply - シークレットはこのボックスがチェックオンされている場合のみ適用される。 このボックスがチェックオンされていない場合、シークレット欄に何を入力しても効果は無く保持されない。この欄はユーザーがRead･Write特権を持つ場合のみ表示される。

Encrypted - シークレット文字列が暗号化される際はこのボックスがチェックオンされていること。 この欄はユーザーがRead･Write特権を持つ場合のみ表示される。

構成不可能なデータ

Secret Configured -このアカウンティング･サーバにシークレットが構成されたことを示す。

コマンド･ボタン

Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければパワーサイクルでは保持されません 。

Remove - 選択されたアカウンティング･サーバを構成から削除する。 このボタンはRead･Write特権ユーザーにのみ利用できる。 変更は保存を実行しなければパワー･サイクル後、保持されない 。

Refresh - デフォルト値は 3600 である。

8.4.4 RADIUS 統計

8.4.4.1 RADIUS 統計

Statistics

Radius Statistics | Server Statistics | Accounting Server Statistics | Clear Statistics

Invalid Server Addresses: 0

Refresh

図： RADIUS 統計

構成不可能なデータ

Invalid Server Addresses - 未知のアドレスから受信された RADIUSアクセス･応答パケットの数。

コマンド･ボタン

Refresh - デフォルト値は 3600 である。

8.4.4.2 サーバ統計

Statistics

Radius Statistics | Server Statistics | Accounting Server Statistics | Clear Statistics

RADIUS Server:
Round Trip Time (secs):
Access Requests:
Access Retransmissions:
Access Accepts:
Access Rejects:
Access Challenges:
Malformed Access Responses:
Bad Authenticators:
Pending Requests:
Timeouts:
Unknown Types:
Packets Dropped:

Refresh

図：RADIUS サーバ統計

選択基準

RADIUS サーバ - 統計を表示するRADIUSサーバのIPアドレスまたはホスト名を選択する。

構成不可能なデータ

Round Trip Time (secs) - このRADIUS認証サーバにより一致した直前のアクセス-応答/アクセス-試行とアクセス-要求の間の 100 分の 1 秒単位の時間間隔。

アクセス要求 - - このサーバに送られたRADIUSアクセス-要求パケット数。 この数は再送信を除く。

Access Retransmissions - このサーバに再度送られたRADIUSアクセス-要求パケット数。

Access Accepts - このサーバから受信された有効と無効パケットを含む、RADIUSアクセス-許可パケット数。

Access Rejects - このサーバから受信された有効と無効パケットを含む、RADIUSアクセス-拒否パケット数。

Access Challenges- このサーバから受信された有効と無効パケットを含む、RADIUSアクセス-試行パケット数。

Malformed Access Responses - このサーバから受信された間違いRADIUSアクセス-応答パケット数。 不正パケットは無効な長さのものを含む。 間違いアクセス-応答には、間違い認証コードまたは間違い署名属性または不明タイプは含まれない。

Bad Authenticators- このサーバから受信された無効認証コードまたは署名属性を含むRADIUSアクセス-応答パケット数。

Pending Requests-まだタイムアウトしていないか応答を受けていないこのサーバをターゲットとするRADIUSアクセス-応答数。

Timeouts- このサーバへの認証タイムアウトの回数。

Unknown Types-認証ポートでこのサーバから受信されたタイプが不明なRADIUSパケット数。

Packets Dropped - 認証ポートでこのサーバから受信され他の理由により落とされたたRADIUSパケット数。

コマンド・ボタン

Refresh - デフォルト値は 3600 である。

8.4.4.3 アカウンティング･サーバ統計

Accounting Server Statistics	
Accounting Server:	
Round Trip Time (secs):	
Accounting Requests:	
Accounting Retransmissions:	
Accounting Responses:	
Malformed Accounting Responses:	
Bad Authenticators:	
Pending Requests:	
Timeouts:	
Unknown Types:	
Packets Dropped:	

Statistics / Radius Statistics / Server Statistics / Accounting Server Statistics / Clear Statistics / Refresh

図：RADIUS アカウンティング･サーバ統計

構成不可統計

Accounting Server- 統計と関連付けられたアカウンティング･サーバを識別する。

Round Trip Time (secs)- このRADIUSアカウンティング･サーバにより一致した直前のアクセス-応答とアクセス-要求の間の 100 分の 1 秒単位の時間間隔。

Accounting Requests- 再送信を除き送信されたRADIUSアカウンティング要求パケット数を表示する。

Accounting Retransmissions- このRADIUSアカウンティング･サーバに再度送られたRADIUSアカウンティング-要求パケット数を表示する。

Accounting Responses- このサーバからアカウンティング･ポートで受信されたRADIUSパケット数を表示する。

Malformed Accounting Responses- このサーバから受信された不正RADIUSアカウンティング-応答パケット数を表示する。 不正パケットは無効な長さのものを含む。 不正認証コードと不明タイプは不正アカウンティング応答に含まれない。

Bad Authenticators- このアカウンティング･サーバから受信された無効な認証コードを含んだRADIUSアカウンティング-応答パケット数を示す。

Pending Requests- まだタイムアウトしていないか応答を受けていないこのサーバをターゲットとするRADIUSアカウンティング-要求数。

Timeouts- このサーバへのアカウンティング･タイムアウトの回数を表示する。

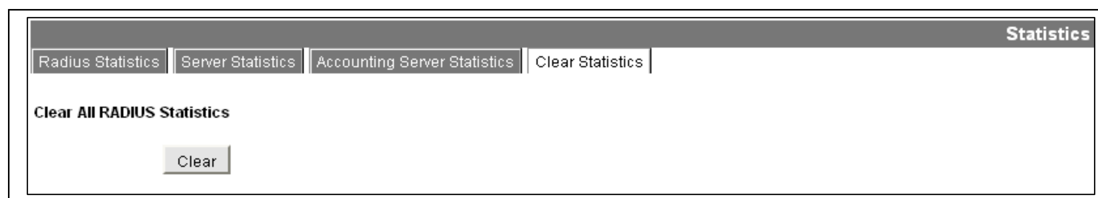
Unknown Types- アカウンティング･ポートでこのサーバから受信されたタイプが不明なRADIUSパケット数を表示する。

Packets Dropped-アカウンティング･ポートでこのサーバから受信され他の理由により落とされたたRADIUSパケット数を表示する。

コマンド･ボタン

Refresh - デフォルト値は 3600 である。

8.4.4.4 統計をクリアする



図：RADIUS 統計のクリア

コマンド･ボタン

Clear All RADIUS Statistics- このボタンはアカウンティング･サーバ、認証サーバ、RADIUS 統計を消去する。

8.4.5 TACACS+

8.4.5.1 コンフィグ

TACACS+

Config | Server Config

Key String (0 to 128 characters): ●●●●●● ☐ Encrypted

Connection Timeout (1 to 30 secs):* 5

* = mandatory

Apply

図：TACACS+ コンフィグ

構成可能データ

Key String - デバイスとTACACS+サーバ間のTACACS+通信のための認証キーと暗号化キーを指定する。 有効な範囲は 0 から-128 までである。 キーはTACACS+サーバで構成された鍵と一致しなければならない 。

Encrypted - キー文字列が暗号化される際はこのボックスがチェックオンされていること。 この欄はユーザーがRead・Write特権を持つ場合のみ表示される 。

Connection Timeout- デバイスとTACACS+サーバ間のTCP接続を確立するために許容される最大秒数。

コマンド・ボタン

Apply - 更新した画面をスイッチへ送ります。 変更はスイッチ上で有効化されますが保存しなければこれらの変更は電源を切ると保持されません。

8.4.5.2 サーバ･コンフィグ

TACACS+

Config	Server Config

TACACS+ Server: Add

IP Address [ ] . [ ] . [ ] . [ ]

* = mandatory

Apply

図：TACACS+ サーバ･コンフィグ

選択基準

TACACS+ Server - データが表示されるまたは構成されるTACACS+サーバを選択する。 add項目を追加するが選択されると、新たなTACACSサーバを構成できる 。

構成可能データ

IP Address - TACACS+サーバのIPアドレスを指定する。
次のIPアドレスを使うことはできない:

- 0.0.0.0
- 255.255.255.255
- 224.xxx.xxx.xxx
- 127.0.0.1

Host Name - 追加されたサーバのホスト名

Priority - TACACS+サーバが使用される順序を指定する。 0 から 65535 までの範囲であることが条件である。

Port -認証ポートを指定する。 0 から 65535 までの範囲であることが条件である。

Key String - デバイスとTACACS+サーバ間のTACACS+通信のための認証キーと暗号化キーを指定する。 有効な範囲は 0 から-128 までである。 キーはTACACS+サーバで使用される暗号化と一致しなければならない 。

Encrypted - キー文字列が暗号化される際はこのボックスがチェックオンされていること。 この欄はユーザーがRead･Write特権を持つ場合のみ表示される 。

Connection Timeout -デバイスとTACACS+サーバ･タイムアウト間の接続前に経過する時間。 値の範囲は 1 から 30 までである。

コマンド･ボタン

Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければパワーサイクルでは保持されません 。

Remove - 選択されたサーバを構成から削除する。

8.4.6 LDAP

8.4.6.1 構成

LDAP

Config

IP Address:* 0 . 0 . 0 . 0

Port(1 to 65535):* 0

Base DN:

RDN attribute:

Bind DN without RDN:

* = mandatory

Apply

図：LDAP コンフィグ

動作

RDN (相対識別名) の属性が"cn"(共有名)であれば、RDN無しの結合DN(識別名) は"dc=test,dc=com"である。ユーザー名は"root"、パスワードは"1234"である。結合DNは"cn=root,dc=test,dc=com"、パスワードは"1234"である。 (OU は"組織単位"の略である。. DCは"ドメイン･コンポーネント"の.略である。.)

構成可能データ

IP Address - LDAPサーバIP、デフォルトは 0.0.0.0。

Port - LDAPサーバTCPポート、デフォルトは 389。

ベースDN - 基底識別名、デフォルトは空白文字列である。

RDN attribute - 結合DNのRDN属性、デフォルトは空白文字列である。

Bind DN without RDN - 部分的結合DNはRDNを除く、デフォルトは空白文字列である。

コマンド･ボタン

Apply - 入力した値でLDAPの構成を更新する。電源を切っても値を保持するには保存しなければなりません。

8.4.7 アクセス制御リスト

8.4.7.1 IPコンフィグ

IP ACLはパケットに対して順番に一致される規則セットから構成される。 パケットが規則の一致基準に合致すると、指定規則動作(許可か拒否) を行い、追加規則は一致上は確認されない。 このメニューではIP ACLが適用されるインターフェイスを指定し、それがインバウンドかアウトバウンド･トラフィックに適用されるかも指定しなければならない。 IP ACLの規則はIP ACL規則構成メニューを使用して指定し生成される 。

Access Control Lists

IP Config | IP Summary | IP Rule Config | MAC Config | MAC Summary | MAC Rule Config | Port Config

IP ACL: Create New Standard IP ACL

IP ACL ID (1 to 99) :* 0

* = mandatory

Apply

Table	Current Size / Max Size
ACL	0 / 100

図 ： アクセス制御リスト IP コンフィグ

選択基準

IP ACL - プルダウン･メニューから選択する。 新たなIPアクセス制御リストを生成する、または、既存IP ACLの構成を更新することができる。

構成可能データ

IP ACL ID - IP ACL IDはIP標準アクセス･リストでは 1 から 99 までの整数、IP拡張アクセス･リストでは 100 から 199 までの整数とする。

構成不可能なデータ

Table - IP ACの現在数と最大数を表示する。

Current Size - IP ACLの現在の数。

Max Size - IP ACLの最大数。

コマンド･ボタン

Apply - 更新した構成をスイッチへ送ります。構成の変更は即時に有効化されます。これらの変更は、保存しなければ電源を切ると保持されません。

Delete - スイッチ構成から現在選択されているACLを削除します。

8.4.7.2 **IPサマリ**

Access Control Lists

IP Config | IP Summary | IP Rule Config | MAC Config | MAC Summary | MAC Rule Config | Port Config

IP ACL ID	Rules	Direction	Slot/Port
1	0		

Refresh

図 : アクセス制御リスト IP サマリ

構成不可能なデータ

IP ACL ID - IP ACLの識別子。

Rules - IP ACLで現在構成されている規則の数。

Direction - IP ACLの制御をうけるパケット・トラフィックの方向。
方法は次のみとなる:

- インバウンド

Slot/Port(s) - IP ACLが適用されるインターフェイス。

コマンド・ボタン

Refresh - 画面上のデータを最新状態に更新する。

8.4.7.3 IP規則コンフィグ

IPアクセス制御リストと構成画面を使用して生成されたIP ACLに規則を構成するためにこれらの画面を使用する。 この画面に表示される内容あh規則構成の現在段階より異なる。 標準か拡張IP ACLをまず選択して規則を構成する。規則識別子、'Action'と'Match Every'パラメータを次に指定する。 'Match Every'が偽に設定されると、新画面が表示されここから一致基準を構成する。

Access Control Lists

IP Config | IP Summary | IP Rule Config | MAC Config | MAC Summary | MAC Rule Config | Port Config

IP ACL: 1
Rule: Create Rule
Rule ID (1 to 10) :* 0
Action: Deny
Match Every: False
* = mandatory

Apply

図 ： アクセス制御リスト IP 規則コンフィグ

選択基準

IP ACL ID - プルダウン･メニューで規則を生成または更新するIP ACLを選択する。

Rule - プルダウン･メニューから既存規則を選択するか、'Create New Rule'(新規則を生成する)を選択する。 ACLのほか新規則を追加するオプション。 新規則は規則の最大数に到達すると生成できない。 規則毎に、パケットは当該規則について真となり指定された規則動作 (許可か拒否) が行われるためには、すべての指定基準と一致しなければならない。

構成可能データ

Rule ID - 規則を識別するための 1 から 10 までの範囲の整数を入力する。 IP ACLは最大 10 規則を持てる。

Action - パケットが規則の基準に合致した場合にとられるべき動作を指定する。 選択内容は許可か拒否である。

Logging - 'True'に設定されると、このACL規則について (デバイス･リソースの 可用性に応じて) ロギングが有効化される。アクセス･リスト･トラップ･フラッグも有効化され た場合、この規則が現在の報告間隔の間に'当たった'回数を示す周期的トラップが生成される。 固定された 5 分の報告間隔がシステム全体で使用される。トラップはACL規則の当たり数が現在の間隔で零の場合には発行されない。 この欄は'Deny'動作には見える。

Assign Queue ID - このIP ACL規則に合格するすべてのパケットを処理するためのハ ードウェア出口キュー識別子を指定する。 キューIDの有効範囲は 0 から 7 までである。 この欄は'Permit'動作には見える。

Mirror Interface -一致するトラフィックの流れがデバイスによる通常の転送に 加えてコピーされる特定の出口インターフェイスを指定する。この欄はリダイレクト･インターフェイスがすでにACL規則について構成された場合には設定できない。 この欄は'Permit'動作にはみなします 。

Redirect Interface ･インターフェイス - 一致するトラフィックの流れがデバイスによる 通常の転送決定を避けて強制される特定の出口インターフェイスを指定する。この欄はミラー･インターフェイスがすでにACL規則について構成された場合には設定できない。 この欄は'Permit'動作にはみなします。

Match Every - プルダウン･メニューからtrue/真かfalse/偽を選択する。 True/真は、すべてのパケットが選択されたIP ACLと規則に一致し、許可または拒否され ることを意味する。この場合、すべてのパケットが規則に一致するので、他の一致基準を構成するオプションは無い。規則について特定の一致基準を構成するためには、規則を削除してから再生成するか、'Match Every'を'False'に再構成して他の一致基準が見えるようにする。

Protocol Keyword - パケットのIPプロトコルが選択されたIP ACL規則の 一致 条件であることを指定する。 とりうる値はICMP、 IGMP、 IP、 TCP、及び、UDPである。 'Protocol Keyword'欄または'Protocol Number'欄のいずれかを使用してIPプロトコル値を一致基準に指定できる。

Protocol Number - パケットのIPプロトコルが選択されたIP ACL規則の一致条件である ことを指定し、プロトコルを番号で識別する。プロトコル番号はIANAに割当てられた基準値であり、1 から 255 までの整数として解釈される。'Protocol Number'欄または'Protocol Keyword'欄のいずれかを使用し てIP プロトコル値を一致基準に指定できる。

Source IP Address -ピリオド区画された十進数表記法によりIP アドレスを入力 して,選択されたIP ACL規則との一致基準としてパケットの送信元IPアドレ スと比較する 。

Source IP Mask - ピリオド区画された十進数表記法によりIPマスクを指定して送信元IPアド レスの値とともに使用する 。

Source L4 Port Keyword - 選択された拡張IP ACL規則の一致条 件としてパケットのソー ス･レイヤー4 ポートを指定する。 これはオプション構成である。 とりうる値はDOMAIN、ECHO、FTP、FTPDATA、HTTP、SMTP、SNMP、TELNET、TFTP、及び、WWWである。これらの各値は対応するポート番号に変換され、これがポート範囲の開始と終了として使用される。

Source L4 Port Number - 選択された拡張IP ACL規則の一致条件としてパケッ トのソー ス･レイヤー4 ポートを指定する。 これはオプション構成である。

Destination IP Address - ピリオド区画された十進数表記法によりIP アドレスを入力して、選択された拡張IP ACL規則との一致基準としてパケットの送信先IPアドレスと比較する 。

Destination IP Mask - ピリオド区画された十進数表記法によりIPマス クを指定し て送信先IPアドレスの値とともに使用する 。

Destination L4 Port Keyword - 選択された拡張IP ACL規則とのターゲ ッ ト･レ イヤー4 ポートの一致基準を指定する。 とりうる値はDOMAIN、ECHO、FTP、FTPDATA、 HTTP、SMTP、 SNMP、TELNET、TFTP、及び、WWWである。これらの各値は対応するポート 番号に変換され、これがポート範囲の開始と終了として使用される。 これはオプション構成である。

Destination L4 Port Number - 選択された拡張IP ACL規則にパケットのタ ーゲット･レイヤー4 ポート番号のの一致条件を指定する。 これはオプション構成である。

Service Type - 拡張IP ACL規則にプルダウン･メニューからサービス･タイプ の一致条件を選択する。 可能な値はIP DSCP、IP precedence、及び、IP TOSであり、これらはIPへ ッダー にある同じサービス･タイプ欄の一致基準を指定する別の方法ではあるが 、それぞれ異なる ユーザー表記法を用いる。 選択後は適切な値を指定できる。

- **IP DSCP Configuration**
  IP DiffServコード･ポイント(DSCP)欄を指定する。 DSCPはIPヘッダー内でサービ ス･タ イプ･オクテットの高い順の 6 ビットとして定義される。 これはオプション構成である。 0 から 63 までの整数を入力する。IP DSCPはドロップダウン･ボックスからDSCPキーワードを 1 個選択して選択される。値を数値を指定して選択する必要がある場合、ドロップダウン･ボックスで'Other'オプションを選択すると、DSCPの数値を入力できるテキストボックスが表示される。
- **IP Precedence Configuration**
  パケット内のIPプレシデンス欄はIPヘッダー内でサービス･タイプ･オクテットの高い順の 3 ビットとして定義される。 これはオプション構成である。 0 から 7 の整数を入力する。

- **IP TOS Configuration**
  パケット内のIP TOS 欄はIPヘッダー内でサービス･タイプ･オクテ ットのすべての8ビットとし て定義 される。 TOSビット値は 00 からFFまでの 16 進数である。 TOSマスク値は 00 か らFF まで の 16 進数である。 TOSマスクはパケット内のIP TOS欄と比較するために使用さ れる TOSビット値内のビット位置を示す。たとえば、ビット 7 が最も有意である、ビット7 および5セットおよびビット 1 クリアを持つIP TOS値を調べるには、TOSビット値 0xA0 とTOS マス ク 0xFFを使用する。 これはオプション構成である。

コマンド･ボタン

Configure - 選択された規則に対応する一致基準を構成する。

Delete - 現在選択されている規則を選択されたACLから削除する。 当該変更は保存を実行しないとパワー･サイクルを一貫しては保持されない。

8.4.7.4 MACコンフィグ

MAC ACLはパケットに対して順番に一致される規則セットから構成される。 パケットが規則の一致基準に合致すると、指定規則動作(許可か拒否) を行い、追加規則は一致上は確認されない。 このメニューではIP ACLが適用されるインターフェイスを指定し、それがインバウンドかアウトバウンド･トラフィックに適用されるかも指定しなければならない。 IP ACLの規則はIP ACL規則構成メニューを使用して指定し生成される 。

Access Control Lists

IP Config | IP Summary | IP Rule Config | MAC Config | MAC Summary | MAC Rule Config | Port Config

MAC ACL: Create New Extended MAC ACL

MAC ACL Name:*

* = mandatory

Apply

Table	Current Size / Max Size
ACL	1 / 100

図 ： アクセス制御リストの MAC コンフィグ

選択基準

MAC ACL - 新たなMACアクセス制御リストを生成できる、または、既存のMAC ACL構成を選択に基づいて更新できる。

構成可能データ

MAC ACL名 - 英数字、数字、ダッシュ、アンダースコア、または、空白文字のみからなるMAC ACL名の文字列を指定する。 名前は英数字で始めること。この欄はACLがすでに生成された場合には現 在選択されているMAC ACLの名前を表示する。

構成不可能なデータ

Table - MAC ACLの現在数と最大数を表示する。

Current Size- MAC ACLの現在の数。

Max Size- MAC ACLの最大数。

コマンド・ボタン

Apply - 更新した構成をスイッチへ送ります。構成の変更は即時に有効化されます。これらの変更は、保存しなければ電源を切ると保持されません。

Rename - 現在選択されているMAC ACLの名前を変える。

Delete - スイッチ構成から現在選択されているMAC ACLを削除します。

8.4.7.5 MACサマリ

Access Control Lists

IP Config | IP Summary | IP Rule Config | MAC Config | MAC Summary | MAC Rule Config | Port Config

MAC ACL Name	Rules	Direction	Slot/Port
abc	0		

Refresh

図 ： アクセス制御リスト MAC サマリ

構成不可能なデータ

MAC ACL名 - MAC ACL識別子。

Rules - MAC ACLに現在構成されている規則の数。

Direction - MAC ACLの制御をうけるパケット・トラフィックの方向。
有効な方向

- インバウンド

Slot/Port(s) - MAC ACLが適用されるインターフェイス。

コマンド・ボタン

Refresh - 画面上のデータを最新状態に更新する。

8.4.7.6 MAC規則コンフィグ

Access Control Lists

IP Config | IP Summary | IP Rule Config | MAC Config | MAC Summary | MAC Rule Config | Port Config

MAC ACL: abc
Rule: Create New Rule
Rule ID (1 to 10) :*
Action: Deny
Match Every: False
* = mandatory

Apply

図 ： アクセス制御リストの MAC 規則コンフィグ

選択基準

MAC ACL - 規則を生成または更新するMAC ACLを選択する。

Rule - 既存の規則を選択するか'Create New Rule'を選択して新規則を追加する。 新規則は規則の最大数に到達すると生成できない。 規則毎に、パケットは当該規則について真となり指定された規則動作 (許可か拒否) が行われるためには、すべての指定基準と一致しなければならない。

構成可能データ

Rule - 規則を識別するための 1 から 10 までの範囲の整数を入力する。

Action - パケットが規則の基準に合致した場合にとられるべき動作を指定する。 選択内容は許可か拒否である 。

Logging - 'True'に設定されると、このACL規則について (デバイス・リソースの可用性に応じて)ロギングが有効化される。 アクセス・リスト・トラップ・フラッグも有効化された場合、この規則が現在の報告間隔の間に'当たった'回数を示す周期的トラップが生成される。 固定された 5 分の報告間隔がシステム全体で使用される。 トラップはACL規則の当たり数が現在の間隔で零の場合には発行されない。 この欄は'Deny'動作には見える。

Assign Queue ID- このACL規則に合格するすべてのパケットを処理するためのハードウェア出口キュー識別子を指定する。 キューIDの有効範囲は 0 から 7 までである。 この欄は'Permit'動作には見える。

Mirror Interface- 一致するトラフィックの流れがデバイスによる通常の転送に加えてコピーされる特定の出口インターフェイスを指定する。 この欄はリダイレクト・インターフェイスがすでにACL規則について構成された場合には設定できない。 この欄は'Permit'動作には見える。

Redirect Interface- 一致するトラフィックの流れがデバイスによる通常の転送決定を避けて強制される特定の出口インターフェイスを指定する。 この欄はミラー・インターフェイスがすでにACL規則について構成された場合には設定できない。 この欄は'Permit'動作みなします 。

CoS - イーサネット・フレームと比較する 802.1pユーザー・プライオリティを指定する。 値の有効範囲は 0 から 7 までである。

CoS - イーサネット・フレームと比較する 802.1pユーザー・プライオリティを指定する。 値の有効範囲は 0 から 7 までである。

ターゲットMAC -

イーサネット・フレームと比較する送信先MACアドレスを指定する。 有効なフォーマットはxx:xx:xx:xx:xx:xxである。

送信先MACアドレス 01:80:C2:xx:xx:xxを使用してBPDUキーワードを指定できる 。

ターゲットMACマスク -

イーサネット・フレームと送信先MACのどのビットを比較するかを指定して送信先MACアドレス・マスクを指定する。 有効なフォーマットはxx:xx:xx:xx:xx:xxである。

送信先MACマスク 00:00:00:ff:ff:ffを使用してBPDUキーワードを指定できる 。

**Ethertype Key - イーサネット・フレームと比較するイーサタイプの値を指定する。
有効な値:**

- **AppleTalk**
- **ARP**
- **IBM SNA**
- **IPv4**
- **IPv6**
- **IPX**
- **MPLS multicast**

- **MPLS unicast**
- **NetBIOS**
- **Novell**
- **PPPoE**
- **Reverse ARP**
- **User Value**

Ethertype User Value - ユーザーが"User Value"をイーサネット・フレームと比較するイーサータイプ・キーとして選択した場合ユーザー定義のカスタマイズ化イーサータイプ値を指定する。 値の有効範囲は 0x0600 から 0xFFFFまでである。

Source MAC - イーサネット・フレームと比較する送信元MACアドレスを指定する。 有効なフォーマットはxx:xx:xx:xx:xx:xxである 。

ソースMACマスク - イーサネット・フレームと比較する送信元MACアドレスを指定する。 有効なフォーマットはxx:xx:xx:xx:xx:xxである 。

VLAN - イーサネット・フレームと比較するVLAN IDを指定する。 値の有効範囲は 0 から 4095 までである。 VLAN範囲またはVLANを構成できる。

Secondary VLAN - イーサネット・フレームと比較する 2 次VLAN IDを指定する。 値の有効範囲は 0 から 4095 までである。 2 次VLAN範囲または 2 次VLANを構成できる。

Match Every - すべて一致のレイヤー2 MACパケットへの指示を指定する。
有効な値:

- **True - すべてのパケットが選択されたACL規則と一致するとみなされることを意味する。**
- **False - すべてのパケットが選択されたACL規則と一致する必要はないことを意味する。**

コマンド・ボタン

Apply - 更新した構成をスイッチへ送ります。構成の変更は即時に有効化されます。これらの変更は、保存しなければ電源を切ると保持されません。

Delete -

現在選択されている規則を選択されたACLから削除する。

当該変更は保存を実行しないとパワー・サイクル後、保持されない 。

8.4.7.7 ポート･コンフィグ

図 ： アクセス制御リスト･ポート･コンフィグ

選択基準

Slot/Port - ACLマッピングのために利用可能なすべての有効なインターフェイスのリストを指定する。 すべての非ルーティング物理インターフェイスとLAGに参加中のインターフェイスがリストアップされる。

Direction - ACLのパケット･フィルタリングの方向を指定する。
有効な方向

- インバウンド

ACL Type - ACLのタイプを指定する。
有効なACLタイプ

- IP ACL
- MAC ACL

IP ACL - すべてのIP ACLのリストを指定する。 この欄はユーザーが"IP ACL"を"ACL Type"として選択した場合にのみ見える。

MAC ACL - すべてのMAC ACLのリストを指定する。 この欄はユーザーが"MAC ACL"を"ACL Type"として選択した場合にのみ見える。

構成可能データ

Sequence Number - オプションのシーケンス番号を指定してこのインターフェイスと方向にすでに割当てられた他のアクセス･リストに対してこのアクセス･リストの順序を示すことができる。番号が低いほどプレシデンスは高いことを示す。シーケンス番号がこのインターフェイスと方向にすでに使用中である場合、指定されたアクセス･リストはそのシーケンス番号を使用して現在付加されたアクセス･リストを置換する。 シーケンス番号がユーザーにより未定義の場合、現在このインターフェイスと方向で使用中の最も高いシーケンス番号より 1 大きいシーケンス番号が使用される。 許可範囲は 1 から 4294967295 である。

構成不可能なデータ

Slot/Port -選択されたインターフェイスを表示する。

Direction - ACLの選択されたパケット･フィルタリングの方向を表示する。

ACL Type - 選択されたインターフェイスと方向に割当てられたACLのタイプを表示する。

ACL Identifier - 選択されたインターフェイスと方向に割当てられたACLを識別するACL番号(IP ACLの場合) あるいはACL 名(MAC ACLの場合) を表示する。

Sequence Number - 選択されたインターフェイスと方向に割当てられた他のACLに対する指定されたACLの順序を意味するシーケンス番号を表示する。

コマンド・ボタン

Apply - 更新した構成をスイッチへ送ります。構成の変更は即時に有効化されます。これらの変更は、保存しなければ電源を切ると保持されません。

Remove - 現在選択されてい ACLインターフェイスの方向マッピングをスイッチの構成から削除する 。

8.4.8 IPフィルター

8.4.8.1 構成

管理IPフィルターはスイッチを構成の変更が許可されているステーションを指定します。5 台までの管理ステーションをスイッチの管理用に選択できる。1 台以上の管理ステーションを定義することを選択すると、IPアドレスにより定義された選択ステーションのみウェブ・マネージャ、Telnetｾｯｼｮﾝ、セキュア・シェル （SSH） またはセキュア・ソケット・レイヤー(SSL)でHTTPSの管理特権を許可される 。

IP Filter

Config

Admin Mode: Disable

Filter Address 1(0.0.0.0 = Disable) :* 0 . 0 . 0 . 0

Filter Address 2(0.0.0.0 = Disable) :* 0 . 0 . 0 . 0

Filter Address 3(0.0.0.0 = Disable) :* 0 . 0 . 0 . 0

Filter Address 4(0.0.0.0 = Disable) :* 0 . 0 . 0 . 0

Filter Address 5(0.0.0.0 = Disable) :* 0 . 0 . 0 . 0

* = mandatory

Apply

図 ：IP フィルター・コンフィグ

選択基準

Admin Mode - IPフィルターの管理モードを有効化か無効化か選択する。

構成可能データ

スイッチ構成の変更が許可されているフィルターアドレス 1～5 のステーション。

コマンド・ボタン

Apply - 更新画面をスイッチへ送る。変更はスイッチですぐに反映しますがこれらの変更は保存しなければ電源を切ると保持されません。

8.4.9 セキュアHTTP

8.4.9.1 構成

Secure HTTP

Config

HTTPS Admin Mode: Disable
TLS Version 1: Enable
SSL Version 3: Enable
HTTPS Port (1 to 65535) :* 443
HTTPS Session Soft Timeout (Minutes) (1 to 60) :* 5
HTTPS Session Hard Timeout (Hours) (1 to 168) :* 24
Maximum Number of HTTPS Sessions (0 to 16) :* 16
* = mandatory

Download Certificates Apply

図 ： セキュア HTTP コンフィグ

構成可能データ

Admin Mode - この選択欄はセキュアHTTPの管理モードを有効化か無効化するため に使用される。 ウェブページが表示されると現在の構成値が表示される。デフォルト値は無効化である。

TLS Version 1 -この選択欄はTLSバージョン 1.0 を有効化か無効化するために使用さ れる。 ウェブ ページが表示されると現在の構成値が表示される。デフォルト値は有効化である。

SSL Version 3 -この選択欄はSSLバージョン 3.0 を有効化か無効化するために使用さ れる。ウェブページが表示されると現在の構成値が表示される。デフォルト値は有効化である。

HTTPSポート番号 - この欄はHTTPSポート番号を設定するために使用する。 その値は 1〜65535 の範囲 でなければばならない。Port443 がデフォルト値である。ウェブページが表示されると現在の 構成値が表示される。

HTTPSセッション･ソフト･タイムアウト - この欄はHTTPSセッションの無動作タイムアウトを設定するために使用される。 その値は 1〜60 分の範囲 で定める。 デフォルト値は 5 分である。ウェブページが表示されると現在の構成値が表示される。

HTTPSセッション･ハード･タイムアウト - この欄はHTTPSセッションのハード･タイム アウトを設定するために使用される。 このタイムアウトはセッションの動作レベルには影響されない。 その値は 1〜168 時間の範囲で定める。デフォルト値は 24 時間である。ウェブページが表示されると現在の構成値が表示される。

最大HTTPSセッション数 - この欄はHTTPSセッションの最大許容数を設定するために使用される。 その値は 0〜16 回の範囲で定める。デフォルト値は 16 である。ウェブページが表示されると現在の構成値が表示される。

コマンド･ボタン

Apply - 更新した画面をスイッチへ送る。変更はスイッチですぐに反映しますが これらの変更は保存 しなけ れば電源を切ると保持されません 。

Download Certificates - SSL証明書のダウンロード用ファイル転送頁へのリンクである。SSL証明書ファイルをダウンロードするにはSSLは管理上無効化されなければならない。

8.4.10 セキュア･シェル

8.4.10.1 構成

Secure Shell

Config

Admin Mode: Disable
SSH Version 1: Enable
SSH Version 2: Enable
SSH Connections Currently in Use: 0
Maximum number of SSH Sessions Allowed: 5
SSH Session Timeout (minutes) (1 to 160) :* 5
* = mandatory

Download Host Keys　Apply

図 ： セキュア･シェル･コンフィグ

構成可能データ

Admin Mode - この選択欄はSSHの管理モードを有効化か無効化するために使用される。 ウェブページが表示されると現在の構成値が表示される。デフォルト値は無効化である。

SSH Version 1 -この選択欄はSSHにプロトコル･レベル 1 を有効化か無効化するために使用される。 ウェブページが表示されると現在の構成値が表示される。デフォルト値は有効化である。

SSH Version 2 - この選択欄はSSHにプロトコル･レベル 2 を有効化か無効化するために使用される。ウェブページが表示されると現在の構成値が表示される。初期値は有効です 。

Maximum Number of SSH Sessions Allowed - この選択欄はスイッチ上で許可された受信SSHセッションの最大数を設定するために使われます。ウェブページが表示されると現在の構成値が表示される。この欄で許容される値の範囲は 0 から 5 までである。

SSHセッションタイムアウト(分) - このテキストフィードはスイッチへ受信されたSSHセッション中止までのタイムアウト値を設定するために使われます。許容される値の範囲は 0 から 160 分までである。

構成不可能なデータ

SSH Connections in Use - システムで現在使用中のSSH接続数を表示する。

コマンド･ボタン

Apply - 更新した画面をスイッチへ送ります。 変更はスイッチ上で有効化されますが保存しなければこれらの変更は電源を切ると保持されません。

Download Host Keys - ホストキーのダウンロード用ファイル転送頁へのリンクである。 SSHキーファイルをダウンロードするにはSSHは管理者により無効化されなければならず、アクティブなSSHセッションがあってはならない 。

8.4.11 Denial-of-Service

8.4.11.1 構成

Denial-of-Service

Config

SIP=DIP: Disable
First Fragment: Disable
TCP Fragment: Disable
TCP Flag: Disable
L4 Port: Disable
ICMP: Disable
Max ICMP Size (0 to 1023):* 512
Max ICMPv6 Size (0 to 1023):* 512
* = mandatory

Apply

図 ： サービス妨害攻撃コンフィグ

構成可能データ

SIP=DIP - プルダウン入力欄の該当行を選択してこのオプションを有効化または無効化する。SIP=DIP DoS防止を有効化すると送信先IPアドレスと同じ送信元ソースIPアドレスを持つパケットをスイッチに破棄させます 。

第 1 フラグメント プルダウン入力欄の該当行を選択してこのオプションを有効化または無効化する。最初の断片のDos防止を有効化すると、構成された最小のTCP Hdrサイズよりも小さいTCP ヘッダーを持つパケットをスイッチに破棄させます。工場側デフォルトは無効化されている。

Min TCP Hdr Size -許可される最小のTCP Hdrサイズを指定します。最初の断片 DoS防止が有効化されていると、この構成された最小のTCP Hdrサイズより小さなTCPヘッダーを持つパケッ トをスイッチは破棄しま す。工場側デフォルトは無効化されている。 ***(注記:この属性はスタックできるイーサネットコネクションブレードで提供されます。)***

TCP Fragment- プルダウン入力欄の該当行を選択してこのオプショ ンを有効化または 無効化する。 TCP断片のDoS防止を有効化すると、1 に等しいIP断片補正値を持つパケットをスイッチに 破棄させます。工場側デフォルトは無効化されている。

TCP Flag-TCPフラッグDoS防止を有効化すると、TCPフラッグ SYNセットと 1024 以 下のT CP ソースポートまたは 0 に設定されたTCPコントロールフラッグセットと 0 に設定されたTCPシーケンス番号またはTCPフラッグFIN、URG、PSHのセットと 0 に設定されたTCPシーケンス番号またはTCPフラグSYNとFINセットの両方等を持つパケットをスイッチに破棄させます。工場側デフォルトは無効化されている。

L4 Port - プルダウン入力欄の該当行を選択してこのオプションを有効化または無効化する。L4 ポートDoS防止を有効化すると、TCP/UDPターゲットポートに等しいTCP/UDPソースポートを持つパケットをスイッチに破棄させます。 工場側デフォルトは無効化されている。

ICMP プルダウン入力欄の該当行を選択してこのオプションを有効化または無効化する。ICMP DoS防止 を有 効化することは、ECHO REQ(ピング)に設定されたタイプと構成されたCMP Pktサイズより大きなサイ ズを持つパケットをスイッチに破棄させます。工場側デフォルトは無効化されている。

Max ICMP Pkt Size -許可された最大のICMP Pktサイズを指定します。 ICMP DoS防止が有効化されていると、スイッチはこの構成されたICMP Pktサイズの最大数より大き なサイズを持 つICMPピングのパケットを破棄します。

Max ICMPv6 Pkt Size -許可された最大限のICMPv6 Pk サイズを指定 します。 ICMP DoS防止が有効化されていると、スイッチはこの構成されたICMPv6 Pktサイズより 大きなサイズを持つICMPv6 ピングパケットを破棄します。工場側デフォルトは無効化されている。

コマンド・ボタン

Apply - 画面の設定をスイッチに更新します。。パワーサイクルしても新しい値をスイッチに保持させるには保存しなければなりません 。

8.5 QoS Menu

8.5.1 差別化サービス

8.5.1.1 グローバル･コンフィグ

パケットは定義された基準に基づいてフィルターされ、処理される。 フィルタリング基準はクラスにより定義される。 処理はポリシーの属性により定義される。 ポリシー属性はクラス毎のインスタンスに基づいて定義され、一致時には当該属性が適用される

構成プロセスはクラスに 1 個またはそれ以上の一致基準を定義することから開始する。 次に 1 個またはそれ以上のクラスがポリシーに追加される。 次にポリシーがインターフェイスに追加される。

パケット処理はパケットについて一致基準をテストすることから開始する。 'all'クラス･タイプのオプションはクラス内の各一致基準はパケットがそのクラスと一致するためにはtrue/真と評定されることが必要であると定義する。 'any'クラス･タイプのオプションは少なくとも 1 個の一致基準はパケットがそのクラスと一致するためにはtrue/真と評定されることが必要であると定義する。 クラスはポリシーに追加された順にテストされる。 ポリシーはポリシー内でクラス一致が発見されたときにパケットに追加される。

Global

Config | DiffServ Wizard

DiffServ Admin Mode: Enable

MIB Table	Current Size / Max Size
Class Table	0 / 32
Class Rule Table	0 / 192
Policy Table	0 / 64
Policy Instance Table	0 / 768
Policy Attributes Table	0 / 2304
Service Table	0 / 112

Apply

図 : DiffServ のグローバル･コンフィグ

選択基準

DiffServ Admin Mode- このモードのオプションをリストし、そこから 1 個を選択できる。デフォルト値は'enable'/有効化である。無効化されている間は、DiffServの構成は保存されていれば保持され、変更できるが、アクティブ化はできない。有効化されると、DiffServserviceはアクティブ化される 。

構成不可能なデータ

Class table - スイッチに許可された合計から構成したDiffServのクラスの数を表示します。

Class Rule table - スイッチに許可された合計から構成されたクラスの規則の数を表示します。

Policy table - スイッチに許可された合計ポリシー数のうち構成されたポリシーの数を表示します。

Policy Instance table - スイッチに許可された合計ポリシークラスインスタンスのうち構成されたポリシークラスインスタンスの数を表示します。

Policy Attributes table - スイッチに許可された合計から構成されたポリシー属性(ポリシークラスインスタンスに付けられた)の数を表示します。

Service table - スイッチに許可された合計から構成されたサービス(特定のインターフェイスのポリシーに付けられた)の数を表示します。

コマンド･ボタン

Apply - 更新した画面をスイッチへ送り変更をスイッチ上で有効化しますが、保存しなければ電源を切るとこれらの変更は保持されません。

8.5.1.2 DiffServウィザード

ウィザードページで選択されたポートへポリシーを追加することにより、スイッチ上のDiffServを有効化します。DiffServは:

– DiffServクラスを生成し、入ってくるトラフィックがクラス·メンバーとなるための要件に合致するかを決めるフィルターとして使用される一致基準を定義する 。

– 次のようにトラフィック·タイプに基づいてDiffServクラスの一致基準を設定する:

- VOIP - UDPプロトコルに一致基準を設定する。
- HTTP - sets match criteria to HTTP ターゲット·ポートに一致基準を設定する。
- FTP - sets match criteria to FTP ターゲット·ポートに一致基準を設定する。
- Telnet - sets match criteria to Telnet ターゲット·ポートに一致基準を設定する。
- Every - すべてのトラフィックに一致基準を設定する。

– DiffServポリシーを生成し、DiffServポリシーを生成されたDiffServクラスに追加する。

– ポリシー化がYES/有りに設定された場合、DiffServポリシー·スタイルはSimple/簡易に設定される。クラス一致基準に合格したトラフィックはアウトバウンド·プライオリティの選択に従い処理される。 アウトバウンド·プライオリティは次のように、合格したトラフィックの処理を構成する:

- High - markdscp efにポリシー化動作を設定する。
- Med - markdscp af31 にポリシー化動作を設定する。
- Low - 送信するポリシー化動作を設定する。

– ポリシー化がNO/無しに設定された場合、すべてのトラフィックが次に指定するようにマークされる:

- High - ipdscp efのポリシー·マークを設定する。
- Med - ipdscp af31 のポリシー·マークを設定する。
- Low - ipdscp beのポリシー·マークを設定する。

– 選択された各ポートは生成されたポリシーに追加される。

Global

Config | DiffServ Wizard

Traffic Type: VOIP

Ports to Include in Config: Encl-CB1/0/1, Encl-CB1/0/2, Encl-CB1/0/3, Encl-CB1/0/4, Encl-CB1/0/5, Encl-CB1/0/6, Encl-CB1/0/7, Encl-CB1/0/8, Encl-CB1/0/9, Encl-CB1/0/10

Policing: YES

Committed Rate(1 - 4294967295)Kbps:* 1

Outbound Priority: High

* = mandatory

Apply

図 : 差別化サービス·ウィザード

選択基準

Traffic Type - トラフィック·タイプはDiffServ クラスを定義するために使用される。 トラフィック·タイプのオプション: VOIP、 HTTP、FTP、Telnet、Every。

ポリシー化 - ポリシー化を有効化するとポリシー設定をDiffServポリシーに追加し、ポリシー割合が適用される 。

Outbound Priority - ポリシー化を有効化するとアウトバウンド･プライオリティはポリシー化に合致するアクションをタイプを定義し、ここに: Highは動作をmarkdscp efに設定し、Medは動作をmarkdscp af31 に設定し、Lowは動作をsendに設定する。 ポリシー化を無効化するとアウトバウンド･プライオリティはポリシーを定義する、ここに: Highはポリシーをipdscp efマークに設定し、 Medはポリシーをipdscp af31 マークに設定し、 Lowポリシーをipdscp beマークに設定する 。

構成可能データ

コンフィグに含めるポート - DiffServポリシーをサポートするために構成できるポートをリストする。 DiffServポリシーは選択されたポートに追加される。

Committed Rate - ポリシー化を有効化すると占有率がポリシーに適用され、ポリシー化動作はconform/一致に設定される。 ポリシー化を無効化すると占有率は適用されず、ポリシーはmarkdscpに設定される 。

コマンド･ボタン

Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければパワーサイクル後、保持されません。

8.5.1.3　クラス･コンフィグ

Class
Class Config　Class Summary
Class Selector:　Create
Class Name:*
Class Type:
* = mandatory
Apply　Cancel

図 ： 差別化サービスのクラス･コンフィグ

選択基準

Class Selector - 新クラスを生成するオプションとともに、これはすべての既存のDiffServｸﾗｽ名をリストし、ここから 1 個選択できる。 この画面の内容はこの欄での選択に応じて変る。 既存クラスが選択された場合画面は構成されたクラスを表示する。 '--create--'が選択された場合、新ｸﾗｽ生成が便利にできる別の画面が表示される。 デフォルトは最初のクラスが生成された状態である。 クラスが存在しない場合、デフォルトは'--create--'/生成するである。

Class Type - プラットフォームでサポートされるすべてのDiffServクラスをリストしここから 1 個を選択できる。 オプション：

- All

新ｸﾗｽが生成されるときのみ、この欄は選択欄である。 クラスの生成後、これは構成されたクラス･タイプを表示する構成不可の欄に変る。

Class Match Selector - これはすべての一致基準をﾘｽﾄし、ここから 1 個を選択して指定されたクラスに追加できる。 一致基準'Any'は、すべてのパケットが指定されたクラスに一致すると見なされ、追加の入力情報は不要であることを意味する。 このドロップダウン･リストの内容は'Reference Class'の一致基準の選択に応じて指定されたクラスについて変る。

– 指定されたクラスが別のクラスを参照しない場合、'Reference Class'の一致基準はドロップダウン一致基準リストに含まれる。 クラスへの参照は'Reference Class'を選択すると確立でき、これは’Add Match Criteria'ボタンを表示させる。

– 指定されたクラスが別のクラスを参照する場合、'Reference Class'の一致基準はドロップダウン一致基準リストに含まれない。 これにより、指定されたクラスが同じタイプの高々1 個の別のクラスを参照できるのでユーザーが別のクラス参照を追加するのを防ぐ。 さらに、画面には現在のクラス参照を削除するために呼び出される'Remove Class Reference'ボタンが表示される。

構成可能データ

Class Name - これは一意にクラスを識別する 1 から 31 文字までの大文字･小文字を区別する英数字文字列である。 'default'というクラス名は予約されており、使用できない。

構成不可能なデータ

Class Type - 新たなクラスが生成されたときのみ、構成されたクラスにタイプを表示する。この欄は選択欄である。クラスの生成後はこの欄は構成不可欄となる。

Match Criteria - 指定されたクラスの構成された一致基準を表示する。

Values - 構成された一致基準の値を表示する。

コマンド・ボタン

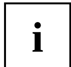
Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければ電力サイクルでは保持されません。

Cancel - 現在選択されているフィルターを取り消す。

Delete - 現在選択されているフィルターを削除する

Rename - 指定されたクラスの名前を変えることができる。

Add Match Criteria -このボタンが呼び出される度に 1 個のみの一致基準を指定できる。 選択された一致基準に基づいて、個々の一致基準画面が表示され値を構成できる。



一致基準はクラスから削除できない。一致基準を削除するためにはクラスを削除しなければならない。

Remove Class Reference -指定されたクラスが別のクラスを参照する場合のみこのボタンが画面に現れる。 指定されたクラスの現在のクラス参照がこのボタンを呼び出すと削除される。

8.5.1.4　クラス･サマリ

図 ： 差別化サービスのクラス･サマリ

構成不可能なデータ

Class Name - 構成されたDiffServクラスの名前を表示する。

Class Type - 構成されたクラスのタイプを表示する。クラス･タイプはプラットフォームに依存する。

Reference Class - 同じタイプの指定されたクラスに参照されるそ

- ALL

のタイプに構成されたクラスの名前を表示する。

コマンド･ボタン

Refresh - 現在選択されているフィルターを更新する。

8.5.1.5　ポリシー･コンフィグ

図 ： 差別化サービスのポリシー･コンフィグ

選択基準

Policy Selector -新クラスを生成するオプションとともに、これはすべての既存のDiffServポリシー名をリストし、ここから1個選択できる。 この画面の内容はこの欄での選択に応じて変る。 既存折シーが選択されると、画面はそのDiffServポリシーのメンバー･クラスを表示する。 'create'が選択された場合、新ポリシーが便利に生成できる別の画面が表示される。 デフォルトは'create'/生成するである。

Policy Type - *In の意味は当該タイプがインバウンド･トラフィック方向に固有であることを示す。 新ポリシーが生成されるときのみ、選択欄に存在する。 ポリシーの生成後、これは構成されたポリシー･タイプを表示する構成不可の欄に変る*　。

Available Class List -既存すべてのDiffServクラス名をリストし、ここから1個選択できる。 この欄は新たなポリシー･クラス･インスタンスが生成されるときのみ選択欄である。 ポリシー･クラス･インスタンスの生成後はこの欄は

構成不可欄となる。

Member Class List -指定されたポリシーのメンバーとして現在定義されている既存すべてのDiffServクラスをリストし、ここから 1 個選択できる。 このリストは新たなクラスがポリシーに追加または削除されると自動的に更新される。 この欄は既存のポリシー・クラス・インスタンスが削除されるときのみ選択欄である。 ポリシー・クラス・インスタンスの削除後はこの欄は構成不可欄となる。

構成可能データ

Policy Name -これは一意にポリシーを識別する 1 から 31 文字までの大文字・小文字を区別する英数字文字列である。

構成不可能なデータ

Policy Type - *In* の意味は当該タイプがインバウンド・トラフィック方向に固有であることを示す。 新ポリシーが生成されるときのみ、この欄は選択欄である。 ポリシーの生成後、これは構成されたポリシー・タイプを表示する構成不可の欄に変る。

Member Class List- 選択された DiffServ ポリシーのメンバー・クラスをすべて表示する。 新たなクラスがポリシーに追加または削除されると自動的に更新される。 この欄は既存のポリシー・クラス・インスタンスが削除されるときのみの選択欄である。 ポリシー・クラス・インスタンスの削除後はこの欄は構成不可欄となる 。

Available Class List -指定されたポリシーのメンバー・クラスをすべて表示する。 新たなクラスがポリシーに追加または削除されると自動的に更新される。 . この欄は新ポリシー・クラス・インスタンスが生成されるときのみの選択欄である。 ポリシー・クラス・インスタンスの生成後はこの欄は構成不可欄となる 。

コマンド・ボタン

Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければパワーサイクル後、保持されません 。

Delete - 現在選択されているフィルターを削除する.

Rename - 指定されたポリシーの名前を変えることができる。

Add Selected Class -ポリシーを指定されたクラスに付加してポリシー・クラス・インスタンスを生成する。

Remove Selected Class -ポリシーを指定されたクラスから切り離してポリシー・クラス・インスタンスを削除する。

8.5.1.6 **ポリシー・サマリ**

Policy Name	Policy Type	Member Classes

図 ： 差別化サービスのポリシー・サマリ

構成不可能なデータ

Policy Name -DiffServポリシーの名前を表示する 。

Policy Type - ポリシー・タイプをIn (インバウンド) として表示する。

Member Classes - ポリシー内の各クラス・インスタンsぬの名前を表示する。

コマンド・ボタン

Refresh - 現在選択されているフィルターを更新する。

8.5.1.7 **ポリシー・クラス定義**

Policy Selector: None
Policy Type:
Member Class List: No Member Classes
Policy Attribute Selector: No Member Classes

図 ： 差別化サービス・ポリシー・クラスの定義

選択基準

Policy Selector - 既存すべてのDiffServポリシー名をリストし、ここから 1 個選択できる。

Member Class List - 指定されたポリシーのメンバーとして現在定義されている既存すべてのDiffServクラスをリストし、ここから 1 個選択できる。 このリストは新たなクラスがポリシーに追加または削除されると自動的に更新され

る。 .

Policy Attribute Selector -このタイプのポリシーでサポートされるすべての属性をリストし、ここから 1 個選択できる。

構成不可能なデータ

Policy Type - 構成されたポリシー･タイプを表示する。

コマンド･ボタン

Configure Selected Attribute -1 個のみの構成基準をこのボタンを呼び出す度に指定できる。 選択された構成基準に基づいて、個々の構成画面が提供される。

8.5.1.8 **ポリシー属性サマリ**

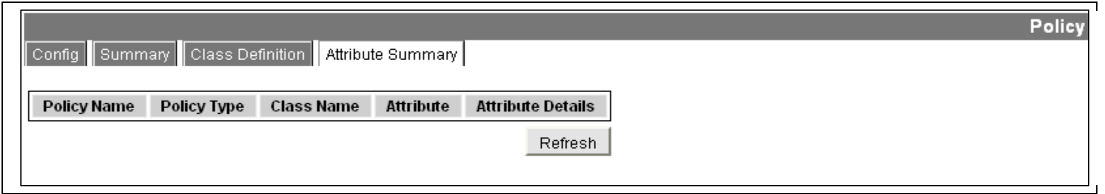


図 : 差別化サービスのポリシー属性サマリ

構成不可能なデータ

Policy Name - 指定されたDiffServポリシーの名前を表示する。

Policy Type - 指定されたポリシー･タイプをIn (インバウンド) として表示する。

Class Name - ポリシーが付加されたDiffServクラスの名前を表示する。

Attribute - ポリシー･クラス･インスタンスに付加された属性を表示する。

Attribute Details - 付加された属性の構成された値を表示する。

コマンド･ボタン

Refresh - 表示されたデータを更新する。

8.5.1.9 サービス･コンフィグ

Service

Config | Summary | Statistics | Detailed Statistics

Slot/Port: Encl-CB1/0/1

Policy In: None

Apply

図 : 差別化サービスのサービス･コンフィグ

選択基準

Slot/Port -インターフェイスを一意に指定するスロット/ポートを選択する。 システムの有効なすべてのスロット番号とポート番号の組合わせをリストする。 Read･Write特権ユーザーではリストに'All'と表示されている場合、すべてのインターフェイスを指定するために選択できる。

Direction - このサービス･インターフェイスのトラフィック方向を選択する。 この選択はスロット/ポートが'All'に指定された場合にはRead･Write特権ユーザーのみ利用できる。

構成可能データ

Policy In - 'In'タイプのすべてのポリシー名をリストし、ここから 1 個選択できる。 'none'/無しが選択された場合、当該ポリシーをこの方向のインターフェイスから切り離す。 インバウンド･サービス･ポリシーの付加がプラットフォームによりサポートされていないRead･Write特権ユーザーにはこの欄は見えない。

構成不可能なデータ

この情報はスロット/ポートが'All'に指定された場合のみ表示される。

Slot/Port -インターフェイスを一意に指定するスロット/ポートを表示する。

Direction - このサービス･インターフェイスのトラフィック方向がインバウンドであることを表示する。

Oper. Status - このサービス･インターフェイスの動作状態、アップかダウンかを表示する。

Policy Name - 付加されたポリシーの名前を表示する。

コマンド･ボタン

Apply - 更新した画面をスイッチへ送る。変更はスイッチでは有効になるがこの変更は保存しなければパワーサイクル後、保持されません 。

8.5.1.10　サービス･サマリ

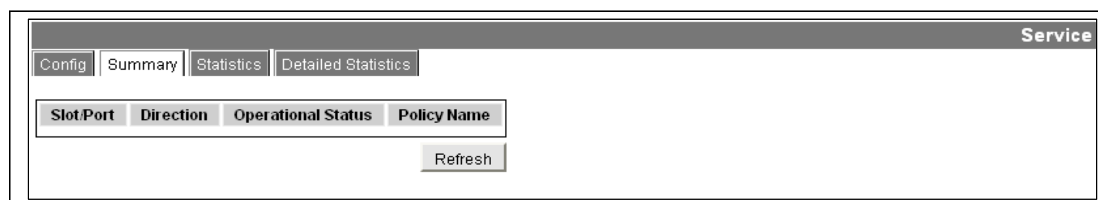


図 : 差別化サービスのサービス･サマリ

構成不可能なデータ

Slot/Port - インターフェイスを一意に指定するスロット/ポートを表示する。

Direction - このサービス･インターフェイスのトラフィック方向がインバウンドであることを表示する。

Oper. Status - このサービス･インターフェイスの動作状態、アップかダウンかを表示する。

Policy Name - 付加されたポリシーの名前を表示する。

コマンド･ボタン

Refresh - 表示されたデータを更新する。

8.5.1.11 サービス統計

この画面はDiffServポリシーがインバウンド･トラフィック方向で付加されたシステム内すべてのインターフェイスについてテーブル形式でサービス･レベル統計情報を表示する。 'Counter Mode Selector'(カウンター･モード･セレクタ)を用いてカウンター表示モードをオクテットまたはパケットに指定する

Slot/Port	Direction	Operational Status

Service

Config | Summary | Statistics | Detailed Statistics

Refresh

図 : 差別化サービスのサービス統計

構成不可能なデータ

Slot/Port - インターフェイスを一意に指定するスロット/ポートを表示する。

Direction - このサービス･インターフェイスのトラフィック方向がインバウンドであることを表示する。

Operational Status - このサービス･インターフェイスの動作状態、アップかダウンかを表示する。

コマンド･ボタン

Refresh - 表示されたデータを更新する。

8.5.1.12 サービス詳細統計

この画面は、インターフェイスと方向により指定される、ポリシーのクラスごとの統計情報を表示する。 'Member Classes'ドロップダウン・リストは指定されたインターフェイスと方向つまり付加されたポリシー (該当する場合) に基づいて内容が決まる。 メンバー・クラス名をハイライトすると指定されたインターフェイスと方向についてのポリシー・クラス・インスタンスの統計情報が表示される。

Service
Config | Summary | Statistics | Detailed Statistics
Slot/Port: None
Direction: None
Policy Name :
Operational Status:
Member Classes: None
Refresh

図 : 差別化サービスのサービス詳細統計

選択基準

Slot/Port -現在インバウンド方向に付加されているDiffServポリシーをもつシステム内の有効なすべてのスロット番号とポート番号の組合わせをリストする。

Direction -インターフェイスのトラフィック方向がインバウンドであるものをリストする。DiffServポリシーが現在付加されている方向のみ表示される。

Member Classes -選択されたポリシー名のメンバーに現在定義されているすべてのDiffServクラスをリストする。 統計を表示するためには 1 回に 1 個のメンバー・クラス名を選ぶ。 選択されたポリシーと関連付けられたクラスが無い場合,リストには何も含まれない 。

構成不可能なデータ

Policy Name - 指定されたインターフェイスと方向に現在付加されているポリシーの名前。

Operational Status -指定されたインターフェイスと方向に現在付加されているポリシーの動作状態。 値はUpかDownである。

コマンド・ボタン

Refresh - 表示されたデータを更新する。

8.5.2 CoS

8.5.2.1 トラストモード

Class of Service

Trust Mode | IP DSCP Mapping | Priority Mapping | Interface | Interface Queue | Interface Queue Status

Slot/Port: Encl-CB1/0/1

Interface Trust Mode: trust dot1p

test

Apply | Restore Defaults

Current 802.1p Priority Mapping	
802.1p Priority	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

*In order to map Traffic class with dot1p go to QoS-->Class of service-->Priority Mapping

図：CoS 信頼モード

選択基準

Slot/Port -すべてのCoS構成可能なインターフェイスを指定する。 "Global"オプションは直前のグローバル構成の設定を表す。 インターフェイス毎にはオーバーライドされていることがある。

Interface Trust Mode - 入口で特定のパケットのマーキングを信頼するかを指定する。
インターフェイス信頼モードは次のうち 1 個のみの値をとりうる；

- untrusted/アントラスト
- trust dot1p/dot1pトラスト
- trust ip-dscp/ip-dscpトラスト

デフォルト値はtrust dot1pである。

構成不可能なデータ

Untrusted Traffic Class - 'untrusted'モードにある場合すべてのトラフィックが向かうトラフィック･クラス(すなわち、キュー) を表示する。 有効な範囲は 0 から 7 である。

Non-IP Traffic Class - 'trust ip-precedence'または'trust ip-dscp'モードにある場合、すべての非IPトラフィックが向かうトラフィック･クラス(すなわち、キュー) を表示する。 有効な範囲は 0 から 7 である。

Current 802.1p Priority Mapping - 現在の 802.1pプライオリティ･マッピングの構成を表示する。

コマンド･ボタン

Apply - 更新した構成をスイッチへ送ります。構成の変更は即時に有効化されます。これらの変更は、保存しなければ電源を切ると保持されません。

Restore Defaults - デフォルト設定に戻す。

8.5.2.2 IP DSCPマッピング

Class of Service

Trust Mode | IP DSCP Mapping | Priority Mapping | Interface | Interface Queue | Interface Queue Status

Slot/Port: Global

IP DSCP Value	Traffic Class
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	1

図 : CoS IP DSCP マッピング

選択基準

Slot/Port - すべてのCoS構成可能なインターフェイスを指定する。 "Global"オプションは直前のグローバル構成の設定を表す。

構成可能データ

IP DSCP Traffic Class- どの内部トラフィック･クラスが対応する IP DSCP値にマップされるかを指定する。 有効な範囲は 0 から 7 である。

構成不可能なデータ

IP DSCP Value - IP DiffServコード･ポイント(DSCP)値を指定する。

コマンド･ボタン

Apply - 更新した構成をスイッチへ送ります。構成の変更は即時に有効化されます。これらの変更は、保存しなければ電源を切ると保持されません。.

Restore Defaults - デフォルト設定に戻す。

8.5.2.3 **プライオリティ･マッピング**

802.1p Priority	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

図：CoS プライオリティ･マッピング

選択基準

Slot/Port -データを表示または構成する物理インターフェイスを選択する。 すべてのポートのパラメータを同じ値に設定するには'All'を選択する。

構成可能データ

Traffic Class - 対応する 802.1pプライオリティをどの内部トラフィック･クラスがマップするかを指定する。

構成不可能なデータ

802.1p Priority - マップされる 802.1pプライオリティを表示する。

コマンド･ボタン

Apply - 画面の設定でスイッチを更新する。電源を切っても、新しい設定をスイッチに保持させるには保存しなければなりません 。

Restore Defaults - デフォルト設定に戻す。

8.5.2.4 インターフェイス

Class of Service

Trust Mode | IP DSCP Mapping | Priority Mapping | Interface | Interface Queue | Interface Queue Status

Slot/Port: Encl-CB1/0/1

Interface Shaping Rate (0 to 100 in increments of 5) :* 0

* = mandatory

Apply　Restore Defaults

図 ：CoS インターフェイス・コンフィグ

選択基準

Slot/Port - すべてのCoS構成可能なインターフェイスを指定する。"Global"オプシ ョンは直前のグ ローバル構成の設定を表す。インターフェイス毎にはオーバーライドされていることがある。

構成可能データ

Interface Shaping Rate - アウトバウンド送信速度を決めるために通常使用する最大許容帯域を指定する。この値はキュー毎の最大帯域構成とは無関係に制御される。 効果的に 2 次レベルのシェーピングとなっている。デフォルト値は 0 である。 値の範囲は 5 ずつ増える 0 から 100 である。 値 0 とは最大速度は無制限であることを意味する。

コマンドボタン

Restore Defaults - デフォルト設定に戻す。

Apply - 更新した構成をスイッチへ送ります。構成の変更は即時に反映されます。これらの変更は、保存しなければ電源を切ると保持されません 。

8.5.2.5 インターフェイス·キュー

図：CoS インターフェイス·キュー·コンフィグ

選択基準

Slot/Port - すべてのCoS構成可能なインターフェイスを指定する。 ”Global”オプションは直 前のグローバル構成の設定を表す。インターフェイス毎にはオーバーライドされていることがある。

Queue ID - インターフェイス毎 (プラットフォーム·ベースで) に利用可能なすべてのキューを指定する。

Scheduler Type- このキューに使用されるスケジューリングの種類を指定する。
スケジューラ·タイプは次のうち 1 個のみである:

- strict
- weighted

デフォルト値はweightedである。

Queue Management Type - このインターフェイスでキューに使用されるキュー管理。これはデバイスがキュー毎に独立的設定をサポートする場合のみ使用される。 キュー管理タイプは次のうち 1 個のみである:

- taildrop

デフォルト値はtaildropである。

構成可能データ

Minimum Bandwidth Allocated - インターフェイス内すべてのキューに個々の最小帯域値の合計を指定する。 合計値は定義された最大 値 100 を超過できない。 選択されたインターフェイスにキューの最小帯域を構成する間にこの値が考慮される。

Minimum Bandwidth - このキューに割当てられる最小保証帯域を指定する。 この値を対応する最大 帯域より高く設定すると自動的に最大帯域の値が同じ値に増加する。 デフォルト値は 0 である。 値の範囲は 5 ず つ増える 0 か ら 100 である。 値 0 は保証最小値がないことを意味する。 選択されたインターフェイスにあるすべての キューの個別最小帯域の合計は定義された最大値 100 を超過できない。

コマンドボタン

Restore Defaults for All Queues - 選択されたインターフェイスのすべてのキュー設定をデフォルト値に戻す。

Apply - 更新した構成をスイッチへ送ります。構成の変更は即時に反映されます。これらの変更は、保存しなければ電源を切ると保持されません 。

8.5.2.6　　**インターフェイス･キュー･ステータス**

Class of Service

Trust Mode | IP DSCP Mapping | Priority Mapping | Interface | Interface Queue | Interface Queue Status

Slot/Port: Encl-CB1/0/1

Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
0	0	weighted	taildrop
1	0	weighted	taildrop
2	0	weighted	taildrop
3	0	weighted	taildrop
4	0	weighted	taildrop
5	0	weighted	taildrop
6	0	weighted	taildrop
7	0	weighted	taildrop

図：CoS インターフェイス･キュー･ステータス

選択基準

Slot/Port - すべてのCoS構成可能なインターフェイスを指定する。 ”Global”オプションは直前のグローバル構成の設定を表す。　インターフェイス毎にはオーバーライドされていることがある。

構成不可能なデータ

Queue ID -　キューIDを指定する。

Minimum Bandwidth - このキューに割当てられる最小保証帯域を指定する。 値 0 は保証最小値がないことを意味する。 選択されたインターフェイスにあるすべてのキューの個別最小帯域の合計は定義された最大値 100 を超過できない。

Scheduler Type - このキューに使用されるスケジューリングの種類を指定する。
スケジューラ･タイプは次のうち 1 個のみである：

- strict
- weighted

Queue Management Type -

このインターフェイスでキューに使用されるキュー管理。 これはデバイスがキュー毎に独立的設定をサポートする場合のみ使用される。

キュー管理タイプは次のうち 1 個のみである：

- Taildrop

8.6 スタック·メニュー



このメニューの機能はスタックできるイーサネットコネクションブレードのみに提供されます。

8.6.1 構成

8.6.1.1 ユニット·コンフィグ

Configuration

Unit Config | Archive Copy

Switch ID:	1
Serial Number:	SQ836MD00041
Role:	Mgmt Switch
Auto Upgrade:	Disable
MAC Address:	00:1E:68:C6:05:82
Hardware Management Preference:	Unassigned
Priority:	Unasssigned
Switch Type:	0xd5140002
Current Status:	Ready
Switch Description:	SB11 L2+ Switch Stacking System - 44 GE, 2 10GE
Detected Code Version:	0.16
Detected Code in Flash:	0.16
Up Time:	26103 seconds

* = mandatory

Apply | Refresh

図 : スタック·ユニット·コンフィグ

選択基準

Switch ID - スタック·ユニットのリストを表示する。 選択されたユニットの詳細が表示される。 スタックの新たなメンバーを再構成できる、管理者のみに見えるCreateオプションもある。

Auto Upgrade - スイッチの自動更新機能を有効化または無効化すること。スイッチをスタックに加える際ファームウェアのバージョンがスタックマスターより低い場合、この機能がスタックマネージャで有効化されていないと自動ファームウェアのアップグレードが実施されます。

Priority - 管理者がこのユニットを他のユニットに優先して管理ユニットにするかを示す 2 バイト欄である。 この設定のデフォルト値は 1 である。 優先レベルを 0 にすると、デバイスは管理ユニットになれない。 この欄はRead Onlyのユーザーには構成できない。

構成可能データ

Switch ID - スタックで選択されたスイッチのスイッチIDを表示します。これは管理ユーザーにより選択されたスイッチのスイッチIDの番号を記憶するために変更できます。この欄は読み取り専門アクセスのユーザーには構成できません。

構成不可能なデータ

Serial Number - スイッチ固有のシリアル番号を表示します 。

Role -選択されたスイッチがマスターかスレーブかを表示します 。

Mac Address - スイッチユニットのMACアドレス。

Hardware Management Preference - このユニットが管理ユニットになれるかを示す 2 バイト欄。 この値が 0 に設定された場合、ユニットは管理ユニット機能をサポートできなくなる。 より値が高いユニットは他の値が低いユニットより管理機能を実行することを優先されることを意味する。 装置メーカーがこの欄は設定する。

Switch Type - 選択されたユニットのハードウェア･タイプを識別する。 これは 32 ビットのデータ欄である。

Current Status - 選択されたユニットの状態を表示する。 とりうる値:

- Ready
- Unsupported
- Code Mismatch
- Config Mismatch
- Not Present
- Code Updating

Switch Description - 装置を識別するために使用される 80 バイトのデータ欄を表示する。

Detected Code Version - 検出されたコードのリリース番号とバージョン番号。

Detected Code in Flash - フラッシュメモリに保存されているコードのリリース番号とバージョン番号を表示する。

Up Time- スイッチの最後の再起動以降の経過時間。

コマンドボタン

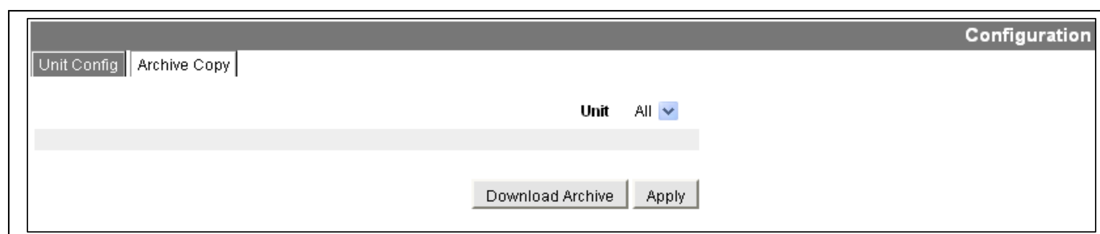
Apply - 画面の値でスイッチを更新する。スイッチ設定を電源を切っても保持させるには保存しなければなりません 。

Delete - スタックから選択されたユニットを削除する。

To be Master - 選択されたユニットをスタック･マスターにする。

Refresh - デフォルト値は 3600 である。

8.6.1.2 **アーカイブ･コピー**



図： スタック･アーカイブ･コピー

選択基準

Unit - 管理ユニット以外のスタックにあるすべてのユニットをリストする。

コマンド･ボタン

Apply - ユニット･セレクタにより指定されたスタック･ユニットに管理ユニットからコードをコピーする。

Download Archive - スイッチへアーカイブファイルをダウンロードします。

8.6.2 情報

8.6.2.1 サマリ

Information

Summary | Port Summary | Port Counters | Port Counters Detail

Switch ID	ID	Role	MAC Address	Priority	Current Status	Code Version
1	Encl-CB1	Mgmt Switch	00:1E:68:C6:05:82	Unassigned	Ready	0.16

Refresh

図 ： スタック･サマリ

構成不可能なデータ

Switch ID - ユニットのIDを表示する。 スタックに許可された最大ユニット数は 8 台である。

ID - ユニットの識別子を表示する。

Role - この欄はユニットがマスターかスレーブかを示す。

MAC Address -スイッチユニットのMACアドレス。

Priority - 管理者がこのユニットを他のユニットに優先して管理ユニットにするかを示す 2 バイト欄である。 この設定のデフォルト値は 1 である。 優先レベルを 0 にすると、デバイスは管理ユニットになれない。 この欄はRead Onlyのユーザーには構成できない。

Current Status - この欄はユニットの状態を示す。 状態を示す 5 個の値がある：

- Ready
- Unsupported
- CodeMismatch
- ConfigMismatch
- NotPresent
- Code Updating

Code Version - この欄はユニットに検出されたコードのバージョンを示す。

コマンド･ボタン

Refresh - デフォルト値は 3600 である。

8.6.2.2 ポート・サマリ

所与のスタックにあるすべてのスタック可能インターフェイスの統計を示す。

Information

Summary | Port Summary | Port Counters | Port Counters Detail

Unit	Interface	Configured Stack-mode	Running Stack-mode	Link Status	Link Speed (Gb/s)
1	Stack 1	N/A	Stack	Link Down	12
1	Stack 2	N/A	Stack	Link Down	12

Refresh

図 : スタック・ポート・サマリ

構成不可能なデータ

Unit - ユニットを表示する。.

Interface - 所与のユニットにあるスタック可能インターフェイスを表示する。

Configured Stack Mode - 所与のインターフェイスに構成されたモードを表示する。 構成されたモードが、ポートが位置するユニットにある、NVRAMに直ちに保存されても、実行時モードは変更されない。

Running Stack Mode - スタック可能インターフェイスの実行時モードを表示する。

Link Status - ポートのリンク・ステータス(UP/DOWN)を表示する。

Link Speed (Gb/s) - スタック・ポートの最高速度を表示する。

コマンド・ボタン

Refresh - ページ上のデータを更新する。

8.6.2.3　**ポート･カウンター**

所与のスタックにあるすべてのスタック可能インターフェイスのカウンターを示す。

Information

Summary | Port Summary | Port Counters | Port Counters Detail

Unit	Interface	Transmit			Recieve		
		Data Rate (Mb/s)	Error Rate (Errors/s)	Total Errors	Data Rate (Mb/s)	Error Rate (Errors/s)	Total Errors
1	Stack 1	0	0	0	0	0	0
1	Stack 2	0	0	0	0	0	0

Refresh

図 ： スタック･ポート･カウンター

構成不可能なデータ

Unit -　ユニットを表示する。.

Interface - 所与のユニットにあるスタック可能インターフェイスを表示する。

送受信統計

- **Data Rate (Mb/s) -** スタック･ポート上の速度概数を表示する。
- **Error Rate (Errors/s)** -スタック･ポート上のエラー頻度概数を表示する。
- **Total Errors -** 起動以降のエラー合計値を表示する。 カウンターはラップできる 。

コマンド･ボタン

Refresh - ページ上のデータを更新する。

8.6.2.4 ポート･カウンターの詳細

特定のスタックにあるスタックできるインターフェイスの診断を表示します。

Information

Summary | Port Summary | Port Counters | Port Counters Detail

Unit	Interface	Statistics
1	Stack 1	RBYT:0 RPKT:0 TBYT:0 TPKT:0 RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0 TAGE:0 TABRT:0
1	Stack 2	RBYT:0 RPKT:0 TBYT:0 TPKT:0 RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0 TAGE:0 TABRT:0

Refresh　Clear Counters

図 ： スタック･ポート･カウンターの詳細

構成不可能なデータ

Unit -　ユニットを表示する。.

Interface - 所与のユニットにあるスタック可能インターフェイスを表示する。

Statistics - デバッグとステータス情報を含むドライバーにより埋められる 3 個のテキスト欄(80 字の文字列)を表示する。

コマンド･ボタン

Refresh - ページ上のデータを更新する。

Clear Counters - スタック･ポートの統計をリセットする。

9 コマンド･レファレンス

コマンド･ライン･インタフェイス (CLI)構文、表記規則、用語をこの節で説明する。 各CLIコマンドを次にサマリーされる構造により説明する。

9.1 CLIコマンド･フォーマット

コマンドには値、パラメータ、またはこれら両方が続く。

例 1

IP address <ipaddr> <netmask> [<gateway>]

- **IP address はコマンド名である。**
- **<ipaddr> <netmask> はこのコマンドに必要な値である。**
- **[<gateway>] はこのコマンドのオプション値である。**

例 2

snmp-server host <loc>

- **snmp-server host はコマンド名である。**
- **<loc> はこのコマンドに必要なパラメータである。**

例 3

clear vlan

- **clear vlan はコマンド名である。**

コマンド

太字の斜体でないフォントは表示されたとおりにタイプすること。

9.2 CLIモード･ベースのトポロジー

パラメータ

パラメータは記述順に依存する。

斜体太字は名前または番号で置換する。 名前パラメータの一部として空白を使用するためには、次のように二重引用符で囲むこと： "System Name with Spaces".

パラメータは、必須の値、オプション値、選択詩、または組合わせでありうる。

- <parameter>. 山括弧＜＞は必須パラメータを括弧とその中の文字列に代えて入力しなければならないことを示す。
- [parameter]. 角括弧[ ]はオプション･パラメータを括弧とその中の文字列に代えて入力できることを示す。
- 選択 1 | 選択 2. ｜は両側パラメータのうち 1 個のみ入力しなければならないことを示す。波括弧 { } はパラメータを 1 個、選択リストから選択しなければならないことを意味する。

値

Ipaddr このパラーターは有効なIPアドレスであり、0 から 255 までの範囲の 4 個の十進バイト数から 構成される。すべてのIPパラメータのデフォルト値は零からなる (すなわち 0.0.0.0)。インタ ーフェ イスIPアドレス 0.0.0.0 は無効である。

macaddr TMACアドレスのフォーマットはたとえば 00:06:29:32:81:40 のようにコロンで 区画された 6 個の 16 進数である。

areaid エリア IDはピリオドで区画された十進数で入力できる (たとえば 0.0.0.1)。 エリアID 0.0.0.0 はバックボーンに予約されている。エリアIDはIPアドレスと同じ形式であるが、IPアドレスとは別個のものである。 サブネット式ネットワークのIPネットワーク番号をエリアIDに使用できる。

routerid T<router id>の値は 4 個の 10 進数字をピリオドで区画した表記とする。(たとえば、0.0.0.1) 0.0.0.0 は無効なルーターIDである。

slot/port このパラメータは有効なスロット番号、及び、有効なポート番号を示す。 たとえば、0/1 はスロ ット番号 0、ポート番号 1 を意味する。<slot/port>欄は標準のスラッシュ (/) で区切られた有効なスロットスロット番号と有効なポート番号からなる。

logical slot/port このパラメータは割当てられた論理スロット番号、及び、論理ポート番号を示す。 ポートチャネル (LAG)の場合に該当する。 オペレータは論理スロット番号、及び、論理ポート番号を使用してポート･チャネルを構成できる。

表記規則

リモート･ホスト、ワークステーション、または、ネットワークへのリンクを定義するためにネットワーク･アドレスは使用される。 ネットワーク･アドレスは次の構文を用いて示される。

アドレス･タイプ	フォーマット	(範囲:
IPAddr	A.B.C.D	0.0.0.0 – 255.255.255.255
MacAddr	YY:YY:YY:YY:YY:YY	16 進数ペア

表; ネットワーク･アドレスの構文

"System Name with Spaces"等の二重引用符はユーザー定義文字列を設定する。 名前のパラメータの一部として空白を使用するには、二重引用符で囲まなければばならない。

しかし空白文字列 (””) はユーザー定義文字列として無効である。 コマンドの完成はコマンド語を一意に識別するために十分なコマンド文字がタイプされたときにコマンドのスペリングを完了する。 コマンドは<enter>をタイプ (コマンド略語) して実行される、または、コマンド語は<tab>または<space bar>をタイプして (コマンドの完成) 完了できる。

'Err'値は要求された値は内部ではアクセス不可であったことを意味する。 これは起きては成らないことであり、不正処理がソフトウェアにあることを示す。

'- - - - -'値は値が不明であることを示す。

注釈

CLIにより、テストまたは構成スクリプトを書くとき、および、より読みやすくするために、コマンド･プロンプトで 1 行注釈をタイプすることができる。 感嘆符('!')文字はコメントの開始をフラッグする。 コメント･フラッグ文字はコマンド行のどこでも単語を開始でき、この文字以降すべての入力内容は無視される。 '!'文字で始まるコマンド行はコメント行として認識されパーサーには無視される。

次にいくつか事例を示す:

```
! Script file for displaying the ip interface
! インターフェイスの情報を表示する
show ip interface 1/0/1 !最初のインターフェイスんついての情報を表示する
! 次のインターフェイスんついての情報を表示する
show ip interface 1/0/2
! スクリプト･ファイルの終了
```

9.3 システム情報と統計的コマンド

9.3.1 show arp

このコマンドはスイッチと他のデバイスのあいだの接続を表示します。アドレス解決プロトコル(ARP)のキャッシュがスイッチと通信しているIPステーションのMACアドレスを識別します。

Syntax
show arp

初期設定

無

コマンド・モード

特権EXEC

表示メッセージ

MAC Address：スイッチが転送かつ/またはフィルタリング情報を持っているユニキャストのMACアドレス。 フォーマットは 6 個の 2 桁の 16 進法の数字でコロンで区切られ、たとえば 00:23:45:67:89:AB形式とします。

IP Address： インターフェイス毎に割当てられたIPアドレス。

Interface： 有効なスロット番号及び有効なポート番号。

9.3.2 show calendar

このコマンドはシステム・クロックを表示する。

Syntax
show calendar

初期設定

無

コマンド・モード

特権EXEC

表示メッセージ

Current Time: システム時刻を表示する

9.3.3 show eventlog

このコマンドはシステムからのエラー・メッセージを含むイベント・ログを表示する。 イベント・ログはシステム・リセット時に消去されない。

Syntax
show eventlog

初期設定

無

コマンド・モード

特権EXEC

表示メッセージ

File： イベントが発生したファイル。

Line： イベントの行番号。

Task Id: イベントのタスクID。

Code: イベント・コード。

Time： 当該イベントの発生時刻。

注記: イベントログの情報はスイッチがリセットされても保持されます。

9.3.4 show running-config

このコマンドはスイッチ上でサポートされている異なるプロトコルパッケージの現在の設定を表示または取得するために使われます。このコマンドはデフォルト値とは異なる値を持つ設定値/構成のコマンドのみ表示または取得します。出力はスクリプトの形式で表示され、同じ条件を持つ別のスイッチを構成するために使用できます。

スクリプト名がある場合、その出力は構成すクリップとにリダイレクトされる。[all]オプションはデフォルト値と同じ値を含む設定や構成によるすべてのコマンドの表示、取得も可能にする。<scriptname>オプションがファイル拡張子".scr"とともに与えられた場合、出力はスクリプト・ファイルにリダイレクトされる。

Syntax
show running-config [all] [<scriptname>] [|]

[all] - デフォルト値と同じ値を含む設定や構成によるすべてのコマンドの表示、取得が可能になる。

[<scriptname>] - 出力を<scriptname>ファイルにリダイレクトする。

[|] - 出力変更子。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

9.3.5 show sysinfo

このコマンドはスイッチ情報のサマリーとサポートされているMIBを表示します。

Syntax
show sysinfo

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

System Description ：このスイッチの識別に使われる文字列。

System Name：スイッチを識別するために使われる名前。

System Location：スイッチの場所を識別するために使われる。 31 個までの英数字が可能です。工場側デフォルト値は空白である。

System Contact：

このスイッチのための連絡先の担当者を識別するために使われるテキストです。31 個までの英数字が可能です。工場側デフォルト値は空白である。

System Object ID： 製造番号。

System Up Time：スイッチの最後の再起動以降の経過時間を日、時間、分で表示します。

MIBs Supported： このエージェントによりサポートされるMIBのリスト。

9.3.6 show system

このコマンドはスイッチのシステム情報を表示します。

Syntax
show system

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

System Description -: このスイッチを識別するために使われるテキスト。

System Object ID: 製造番号

システム情報

System Up Time:最後のスイッチの再起動以降の経過時間を日、時、分で表示。

System Name : スイッチを識別するために使われる名前。

System Location: スイッチの場所を識別するために使われるテキスト。31 個までの英数字が可能です。工場側デフォルト値は空白である。

System Contact : このスイッチのための連絡先の担当者を識別するために使われるテキストです。31 個までの英数字が可能です。工場側デフォルト値は空白である。

MAC Address:インバンド接続のために使用されるMACアドレス 。

Web Server: ウェブ・サーバ機能を有効化/無効化するために表示される。

Web Server Port: ウェブ・サーバのhttpポートを表示する

Web Server Java Mode:ヘッダーフレームのJAVAアプレットへのアクセスを許可すべきかどうかを指定します。有効とはアプレットが見えることです。工場出荷時のデフォルトは無効化です。

Protocol Current: 現在使用中のネットワーク・プロトコルを示す。 オプションはbootp | dhcp | noneである。

DHCP Client Identifier TEXT:このスイッチのためのDCHPクライアント識別子

9.3.7 show hardware

このコマンドはスイッチの全項目情報を表示します。

Syntax
show hardware

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

System Description : このスイッチの製品名を識別するために使われるテキスト

Machine Type: 重要製品データにより定義されたマシン・モデルを指定する。

Machine Model：重要製品データにより定義されたマシン・モデルを指定する。

Serial Number: このスイッチのシリアル番号 。

Label Revision Number：このスイッチのラベル改訂シーケンス番号は製造の目的に使われます。

Part Number： パーツ製造番号。

Hardware Version: このスイッチのハードウェアのバージョン。4 部に分かれています。第 1 バイトは大きなバージョンで第 2 バイトは小さなバージョンを表します。

Loader Version - スイッチ上で現在稼働しているローダーのコードの公開バージョンメンテナンス番号です。たとえば、公開が 1 でバージョンが 2 であればフォーマットは「1.2.」となります。

Boot Rom Version - スイッチ上で現在稼働しているブートROMのコードの公開バージョンメンテナンス番号です。たとえば、公開が 1 でバージョンが 2 であればフォーマットは「1.2.」となります。

Operating Code Version：スイッチ上で現在稼働しているコードの公開バージョンメンテナンス番号です。たとえば、公開が 1 でバージョンが 2 であればフォーマットは「1.2.」となります。

（注記: 下記の情報はSFP/SFP+モジュールをプラグインすると表示される。

Module 1 : 検出さたモジュール・タイプ、たとえば、SFPまたはSFP+

Status： この検出されたモジュールの状態、たとえばOKまたはNot Supported。

ギガビット・イーサネット準拠コード：SFP/SFP+トランシーバのベンダー名は、会社の正式名、会社名の一般に通用している略称

Vendor Name: メーカー名。

Vendor Part Number： SFP+トランシーバのベンダーが割当てたパーツ番号。

Vendor Serial Number: ベンダーが割当てた連番。

Vendor Revision Number：ベンダーが割当てたリビジョン番号。

Vendor Manufacturing Date: ベンダーの製造日。

Additional Packages: このシステムに一体化された追加パッケージを表示する。

9.3.8 show version

このコマンドはスイッチのバージョン情報を表示します。

Syntax
show version

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Serial Number: このスイッチのシリアル番号

Hardware Version: このIBP.のハードウェア・バージョン。このスイッチのハードウェアバージョン。4 部に分かれています。第 1 バイトは大きなバージョンで第 2 バイトは小さなバージョンを表します。

Number of ports : このスイッチではいくつのポートがサポートされているか。

Label Revision Number: このスイッチのラベル改訂シーケンス番号は製造の目的に使われます。

Part Number: パーツ製造番号。

Machine Model: 機種のうちの型式。

Loader Version: スイッチ上で現在稼働しているローダーのコードの公開バージョンメンテナンス番号です。たとえば、公開が 1 でバージョンが 2 であればフォーマットは「1.2.」となります。

Operating Code Version: スイッチ上で現在稼働しているコードの公開バージョンメンテナンス番号です。たとえば、公開が 1 でバージョンが 2 であればフォーマットは「1.2.」となります。

Boot Rom Version: スイッチ上で現在稼働しているブートROMのコードの公開バージョンメンテナンス番号です。たとえば、公開が 1 でバージョンが 2 であればフォーマットは「1.2.」となります。

9.3.9 show tech-support

このコマンドはトラブルシューティングに必要なスイッチ情報を表示します。

Syntax
show tech-support

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

9.3.10 show loginsession

このコマンドはスイッチへのTelnet とシリアルポート接続を表示します。

Syntax
show loginsession

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

ID: ログイン・セッションID

User Name: シリアルポートまたはTelnet によりユーザーがログインのために使う名前。 新しいユーザーは空欄のエントリへ名前を入力しスイッチに追加されます。ユーザー名は 8 文字までが可能で、大文字小文字を区別しません。 工場出荷時デフォルトでは 2 人のユーザー、すなわち管理者とゲストがいます。

Connection From: Telnetクライアント・マシンまたはシリアルポート接続のEIA-232 のIPアドレス。

アイドル時間: このセッションがアイドルである時間。

Session Time: このセッションの接続されている合計時間。

Session Type: セッション・タイプを示す: telnet、シリアル、または、SSH。

9.4 デバイス構成コマンド

9.4.1 インターフェイス

9.4.1.1 show interface status

このコマンドはシステムのポート監視情報を表示する。

Syntax
show interface status {<slot/port> | all}

<slot/port> - 必要なインターフェイス番号である。

all - このパラメータはすべてのインターフェイスについて情報を表示する。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Intf: 物理スロットと物理ポート。

Type:空白でない場合、この欄は当該ポートが特別な種類のポートであることを示す。 とりうる値:

Source- ポートは監視ポートである。

PC Mbr - このポートはポートチャネルのメンバーである(LAG)。

Dest - このポートはプローブ・ポートである。

管理モードポート制御管理ステートを選択する。 ポートはネットワークに許可されるには有効化されていなければならない。 – ポートは有効化または無効化できる。 デフォルト設定は有効化されている。 .

E-Keying Status: E-KEY機能の状態を示す 。

Physical Mode: 必要なポート速度と二重モードを選択する。 自動ネゴシエーションのサポートを選択すると、二重モードと速度が自動ネゴシエーションにより設定される。 ポートの最高性能 (全二重で 100Mbps)が通知されることに注意する。 さもなければ、このオブジェクトはポートの二重モードと転送速度を決める。 工場側デフォルトはautoである。

Physical Status: ポート速度と二重モードを示す。

リンク・ステート リンクがアップかダウンかを示す。

Link Status: リンクがアップかダウンかを示す。

Link Trap:

このオブジェクトはリンク・ステータスが変化したときトラップを送るかを定義する。　デフォルト設定は有効化されている。

LACP Mode: このポートでLACPを有効化するか無効化するかを表示します。

Flow Mode: フロー制御モードを表示する。

Capabilities Status: インターフェイスの機能を表示する。

9.4.1.2 show interface counters

このコマンドは特定のインターフェイスまたはすべてのインターフェイスの統計サマリを表示する。

Syntax
show interface counters {<slot/port> | all}

<slot/port> - 必要なインターフェイス番号である。

all - このコマンドはすべてのインターフェイスについて統計情報を表示する。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

引数が'<slot/port>'のときの表示パラメータ:

Packets Received Without Error:プロセッサに受信されたパケット総数 (ブロードキャスト・パケットとマルチキャスト・パケットを含む)

Packets Received With Error:エラーが有るため高レイヤー・プロトコルにデリバリされえなかったインバウンド・パケット数

Broadcast Packets Received:ブロードキャスト・アドレスにダイレクトされた受信パケット総数 これにはマルチキャスト・パケットが含まれないことに注意する。

Packets Transmitted Without Error:インターフェイスから送信されたパケットの総数。

Transmit Packets Errors:エラーのため送信できなかったアウトバウンド・パケット数。

Collisions Frames:当該イーサネット・セグメントでのコリジョン総数の推計値 。

Time Since Counters Last Cleared: このポートの統計が最後にクリアされて以降経過した時間を日数、時間、分、秒で示したもの 。

引数が'all'のときの表示パラメータ:

Interface: 物理スロットと物理ポート、または、論理スロットと論理ポート。

Summary: すべてのポートの統計の合算。

Packets Received Without Error:受信されたパケット総数 (ブロードキャスト・パケットとマルチキャスト・パケットを含む)。

Packets Received With Error: エラーが有るため高レイヤー・プロトコルに送信されなかったインバウンド・パケット数

Broadcast Packets Received:ブロードキャスト・アドレスにダイレクトされた受信パケット総数 これにはマルチキャスト・パケットが含まれないことに注意する。

Packets Transmitted Without Error: 送信されたパケット総数。

Transmit Packets Errors:エラーのため送信できなかったアウトバウンド・パケット数。

Collisions Frames:当該イーサネット・セグメントでのコリジョン総数の最善推計値。

このコマンドは引数に基づいて特定のポートまたはすべてのCPUトラフィックの詳細統計を表示する。

Syntax
show interface counters detailed {<slot/port> | switchport}

<slot/port> -必要なインターフェイス番号である。

switchport - このパラメータはスイッチ全体かすべてのインターフェイスを指定します。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

引数が'<slot/port>'のときの表示パラメータ:

Total Packets Received (Octets):ネットワークで受信された(失敗したパケットにあるものを含む)データ・オクテット総数（フレーム・ビットを除きFCSオクテットを含む）. このオブジェクトはイーサネット使用度の適度な推計値として使用できる。 より高精度が必要な場合、etherStatsPktsとetherStatsOctetsオブジェクトが共通間隔の前後にサンプルされる必要がある。 この方程式の結果は 0 から 100 パーセントまでの尺度によるイーサネット・セグメントの使用率パーセントである使用率の値である。

Packets Received 64 Octets: 長さ 64 オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 65-127 Octets: 長さ 65 と 127 オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 128-255 Octets: 長さ 128 と 255 オクテットの受信された（フレーム・ビットを除きFCSオクテットを含む).パケット総数（失敗したパケットを含む）。

Packets Received 256-511 Octets: 長さ 256 と 511 オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 512-1023 Octets: 長さ 512 と 1023 オクテットの受信された（フレーム・ビットを除きFCSオクテットを含む).パケット総数（失敗したパケットを含む)。

Packets Received 1024-1518 Octets -

長さ 1024 と 1518 オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received >1522 Octets: 長さ 1522 オクテット超の受信され(フレーム・ビットを除きFCSオクテットを含む)、良好に形成されたパケット総数。

Packets RX and TX 64 Octets:

長さ 64 オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets RX and TX 65-127 Octets -長さ 65 と 127 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む）。

Packets RX and TX 128-255 Octets: 長さ 128 と 255 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 256-511 Octets : 長さ 256 と 511 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 512-1023 Octets : 長さ 512 と 1023 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 1024-1518 Octets : 長さ 1024 と 1518 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 1519-2047 Octets:

長さ 1519 と 1522 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む）。

Packets RX and TX 2048-4095 Octets:

長さ 2048 と 4095 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む）。

Packets RX and TX 4096-9216 Octets:

長さ4096と9216オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Total Packets Received Without Error

Unicast Packets Received: 高レベル・レイヤー・プロトコルに送信されたユニキャスト・パケット数 。

Multicast Packets Received:マルチキャスト・アドレスにダイレクトされた受信された良好なパケットの総数。 この総数にはブロードキャスト・アドレスにダイレクトされたパケットは含まれないことに注意する。

Broadcast Packets Received:ブロードキャスト・アドレスにダイレクトされた受信された良好パケットの総数。 これにはマルチキャスト・パケットが含まれないことに注意する。

Total Packets Received with MAC Errors

Jabbers Received:

長さ 1518 オクテット超の受信され(フレーム・ビットを除きFCSオクテットを含む).、良好に形成され、さらに整数のオクテット数による失敗したフレーム・チェック・シーケンス(FCSエラー)または非整数のオクテット数による失敗したFCS(アラインメント・エラー)があるパケット総数。 このジャバー定義はIEEE-802.3 セクション 8.2.1.5 (10BASE5) とセクション 10.3.1.4 (10BASE2)の定義とは異なる。 この文書ではジャバーをパケットが 20msを超える条件として定義する。ジャバー検出許容範囲は 20msから 150msである。

Undersize Received:

長さ 64 オクテット未満の受信され(フレーム・ビットを除きFCSオクテットを含む)、正常なCRCによるパケット総数 。

Fragments Received:

長さ 64 オクテット未満の受信され(フレーム・ビットを除きFCSオクテットを含む)、エラーCRCがあるパケット総数。

Alignment Errors: 64 ビット以上 1518 以下の長さ(フレーム・ビットを除きFCSオクテットを含む) であるがオクテット数が整数ではない不正FCSがある受信されたパケット総数。

FCS Errors: 64 ビット以上 1518 以下の長さ(フレーム・ビットを除きFCSオクテットを含む) であるがオクテット数が整数の不正FCSがある受信されたパケット総数。

Overruns:このポートが受信パケットにより過負荷状態となり、流入パケットに対応できなくなったために破棄されたフレーム総数。

MTU Errors:

このポートが流入パケットによりMTUより大きかったため破棄されたフレーム総数。

Total Packets Received with MAC Errors

Total Packets Transmitted (Octets):

Packets Transmitted 64 Octets: 長さ 64 オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Transmitted 65-127 Octets: 長さ 65 と 127 オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Transmitted 128-255 Octets: 長さ 128 と 255 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 256-511 Octets: 長さ 256 と 511 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 512-1023 Octets: 長さ 512 と 1023 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 1024-1518 Octets -長さ 1024 と 1518 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Max Frame Size: 最大フレーム・サイズを表示する。

Total Packets Transmitted Successfully

Unicast Packets Transmitted:高レイヤー・プロトコルがユニキャスト・アドレスへの送信を要求したパケット総数で破棄されたものも送られなかったものも含む。

Multicast Packets Transmitted:高レイヤー・プロトコルがマルチキャスト・アドレスへの送信を要求したパケット総数で破棄されたものも送られなかったものも含む。

Broadcast Packets Transmitted: 高レイヤー・プロトコルにブロードキャスト・アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む。

Tx Oversized:最大許容フレーム・サイズを超過したフレーム総数。 このカウンターは 1 秒当たり 10 メガビット出 1 秒当たり 815 カウントの最大インクリメント率がある。

Total Transmit Errors

FCS Errors: 64 ビット以上 1518 以下の長さ(フレーム・ビットを除きFCSオクテットを含む) であるがオクテット数が整数の不正FCSがある送信されたパケット総数。

Underrun Errors: 送信FIFOバッファーがフレーム送信中に空になったため破棄されたフレーム総数

Total Transmitted Packets Discards

Single Collision Frames:送信がコリジョン 1 回で妨害された特定インターフェイス上で送信が完了したフレーム数 。

Multiple Collision Frames: 送信が 1 回以上のコリジョンで妨害された特定インターフェイス上で送信が完了したフレーム数 。

Excessive Collisions:過度のコリジョンにより特定インターフェイスでの送信障害を起こしたフレーム数。

GVRP PDUs Received : GARPレイヤーで受信したGVRP PDUのカウント

GVRP PDUs Transmitted: GARPレイヤーから送信されたGVRP PDUのカウント

GVRP Failed and Registrations: GVRPの登録を試みて完了できなかった回数

GMRP PDUs received: GARPレイヤーから受信したGMRP PDUのカウント

GMRP PDUs Transmitted: GARPレイヤーから送信されたGMRP PDUのカウント。

GMRP Failed Registrations: GMRPの登録試行が完了しなかった回数。

STP BPDUs Transmitted: 送信されたスパニングツリープロトコルのデータ・ユニット。

STP BPDUs Received: 受信したスパニングツリープロトコルのデータ・ユニット。

RSTP BPDUs Transmitted: 送信された高速スパニングツリープロトコル・ブリッジのデータ・ユニット。

RSTP BPDUs Received: 受信した高速スパニングツリープロトコル・ブリッジのデータ・ユニット。

MSTP BPDUs Transmitted:送信されたマルチプル・スパニングツリープロトコル・ブリッジのデータ・ユニット。

MSTP BPDUs Received: 受信したマルチプル・スパニングツリープロトコル・ブリッジのデータ・ユニット。

Time Since Counters Last Cleared:このポートの統計が最後にクリアされて以来経過した時間を日数、時間、分、秒で示したもの。

引数が'switchport'のときの表示パラメータ:

Total Packets Received (Octets): プロセッサにより受信されたデータ・オクテット総数 (フレーム・ビットを除きFCSオクテットを含む)。

Packets Received Without Error: プロセッサに受信されたパケット総数 (ブロードキャスト・パケットとマルチキャスト・パケットを含む) 。

Unicast Packets Received: 高レベル・レイヤー・プロトコルにデリバリされたユニキャスト・パケット数。

Multicast Packets Received: マルチキャスト・アドレスにダイレクトされた受信されたパケットの総数。 この総数にはブロードキャスト・アドレスにダイレクトされたパケットは含まれないことに注意する。

Broadcast Packets Received: ブロードキャスト・アドレスにダイレクトされた受信パケット総数。 これにはマルチキャスト・パケットが含まれないことに注意する。

Receive Packets Received: 高レイヤー・プロトコルへの送信を妨げるエラーが検出されなくても廃棄されたインバウンド・パケット数。 パケット廃棄の考えうる理由はバッファー容量を空けるためなど 。

Octets Transmitted - インターフェイスから送信された、フレーム文字を含むオクテット総数

Packets Transmitted Without Errors - インターフェイスから送信されたパケット総数

Unicast Packets Transmitted - 高レイヤー・プロトコルにサブネットワーク・ユニキャスト・アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む

Multicast Packets Transmitted - 高レイヤー・プロトコルにマルチキャスト・アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む

Broadcast Packets Transmitted - 高レイヤー・プロトコルにブロードキャスト・アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む。

Transmit Packets Discarded - 高レイヤー・プロトコルへの送信を妨げるエラーが検出されなくても廃棄されたアウトバウンド・パケット数。 パケット廃棄の考えうる理由はバッファー容量を空けるためなど 。

Most Address Entries Ever Used -再起動以降にスイッチに学習された転送データベース･アドレステーブルのエントリの最大数 Address Entries Currently in Use: このスイッチの転送データベース･アドレステーブルに学習された静的エントリの数 。

Maximum VLAN Entries - このスイッチに許可された仮想LAN(VLAN)の最大数。

Most VLAN Entries Ever Used -最後の再起動以降このスイッチでアクティブだったVLANの最大数。

Static VLAN Entries-静的生成スイッチで現在アクティブなVLANエントリの数。

Dynamic VLAN Entries: GVRP登録で作成されたこのスイッチ上の現在アクティブなVLANエントリの数。

VLAN Deletes -最後の再起動以降に作成され、削除されたこのスイッチ上のVLANの数。

Time Since Counters Last Cleared - このスイッチの統計が最後にクリアされて以降の経過時間を日、時、分、秒で表示。

9.4.1.3 show interface switch

このコマンドはすべてのCPUトラフィックの統計サマリを表示する。

Syntax
show interface switch

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Packets Received Without Errors- プロセッサに受信されたパケット総数（ブロードキャスト・パケットとマルチキャスト・パケットを含む）

Broadcast Packets Received: ブロードキャスト・アドレスにダイレクトされた受信パケット総数 これにはマルチキャスト・パケットが含まれないことに注意する。

Packets Received With Error: エラーが有るため高レイヤー・プロトコルに送信されなかったインバウンド・パケット数

Packets Transmitted Without Error: インターフェイスから送信されたパケットの総数。

Broadcast Packets Transmitted: 高レイヤー・プロトコルがブロードキャスト・アドレスへの送信を要求したパケット総数で破棄されたものも送られなかったものも含む。

Transmit Packets Errors: エラーのため送信できなかったアウトバウンド・パケット数。

Address Entries Currently in Use: 学習した静的なエントリも含めてスイッチで現在アクティブな転送データベース・アドレステーブルのエントリの合計数 。

VLAN Entries Currently In Use: 現在VLANテーブルを使用中のVLANエントリの数

Time Since Counters Last Cleared: このスイッチの統計が最後にクリアされて以降の経過時間を日、時、分、秒で表示。

9.4.1.4 interface

このコマンドはインターフェイス構成モードに入るために使用される。

Syntax
interface <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.4.1.5 interface range

このコマンドによりインターフェイスレンジの設定モードに入ります。

Syntax
interface range {<slot/port> [- <slot/port>]} [, {<slot/port> [- <slot/port>]} [, {<slot/port> [- <slot/port>]} [, {<slot/port> [- <slot/port>]} [, {<slot/port> [- <slot/port>]}]]]]

<slot/port> -必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.4.1.6 speed-duplex

このコマンドによりインターフェイスにspeedとduplexのモードを設定します。

Syntax
speed-duplex {10 | 100} {full-duplex | half-duplex}

100 - 100BASE-T

10 - 10BASE-T

full-duplex -全二重

half-duplex -半二重

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりインターフェイスにspeedとduplexのモードを設定します。

Syntax
speed-duplex all {10 | 100} {full-duplex | half-duplex}

100 - 100BASE-T

10 - 10BASE-T

full - duplex - 全二重

half - duplex - 半二重

all - このコマンドはすべてのインターフェイスを表します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.4.1.7 negotiate

このコマンドによりポートの自動ネゴシエーションを有効化します。デフォルト値は有効化です。

Syntax
negotiate no negotiate

no – このコマンドによりポートの自動ネゴシエーションを無効化します。

初期設定

有効化

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりすべてのインターフェイスの自動ネゴシエーションを有効化します。デフォルト値は有効化です。

Syntax
negotiate all no negotiate all

all - このコマンドはすべてのインターフェイスを表します。

no - このコマンドによりすべてのインタフェイスの自動ネゴシエーションを無効化します。

初期設定

有効化

コマンド・モード

グローバル・コンフィグ

9.4.1.8 capabilities

このコマンドによりインターフェイスレンジの特定の機能を設定します 。

Syntax
capabilities {{10 | 100 } {full-duplex | half-duplex}} | {1000 full-duplex } no capabilities {{10 | 100 } {full-duplex | half-duplex}} | {1000 full-duplex }

10 - 10BASE-T

100 - 100BASE-T

1000 - 1000BASE-T

full-duplex - 全二重

half-duplex - 半二重

no - このコマンドによりポートの自動ネゴシエーションを無効化します。

初期設定

10 半二重、10 全二重、100 半二重、100 全二重、1000 全二重

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりすべてのインターフェイスレンジの機能を設定します。

Syntax
capabilities all {{10 | 100} {full-duplex | half-duplex}} | {1000 full-duplex } no capabilities all {{10 | 100} {full-duplex | half-duplex}} | {1000 full-duplex }

10 - 10BASE-T

100 - 100BASE-T

1000 - 1000BASE-T

full-duplex - 全二重

half-duplex - 半二重

all - このコマンドはすべてのインターフェイスを表します。

no - このコマンドによりポートの自動ネゴシエーションを無効化します。

初期設定

10 半二重、10 全二重、100 半二重、100 全二重、1000 全二重

コマンド・モード

グローバル・コンフィグ

9.4.1.9 storm-control flowcontrol

このコマンドはスイッチの 802.3xフロー制御を有効化します。

注記:このコマンドは全二重モードのポートのみに適用されます。

Syntax
storm-control flowcontrol no storm-control flowcontrol

no – このコマンドはスイッチの 802.3xフローを無効化します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

このコマンドにより特定のインターフェイスの 802.3xフロー制御を有効化します。

注記:このコマンドは全二重モードのポートのみに適用されます。

Syntax
storm-control flowcontrol no storm-control flowcontrol

no – このコマンドにより特定のインターフェイスの 802.3xフロー制御を無効化します。

初期設定

無効

コマンド・モード

インターフェイス・コンフィグ

9.4.1.10 **shutdown**

このコマンドによりポートを無効化します。

Syntax
shutdown no shutdown

no – このコマンドによりポートを有効化します。

初期設定

有効

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりすべてのインターフェイスレンジの機能を設定します。

Syntax
shutdown all no shutdown all

all - このコマンドはすべてのインターフェイスを表します。

no – このコマンドによりすべてのポートを有効化します。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

9.4.1.11 **MDI/MDIX**

このコマンドにより物理ポートのMDI/MDIXモードを設定します。

Syntax
mdi {auto | across | normal} no mdi

auto - MDI 強制自動モード

across - MDIアクロスモード

normal - MDIノーマルモード

no – このコマンドによりmdiをデフォルト設定に戻します。

初期設定

ノーマル

コマンド・モード

インターフェイス・コンフィグ

9.4.2 L2 MACアドレスとマルチキャスト転送データベーステーブル

9.4.2.1 show mac-addr-table

このコマンドにより転送データベースエントリを表示します。パラメータをつけずにコマンドを入力するとテーブル全体が表示されます。任意のallパラメータを入力した場合も同様です。管理者がMACアドレスを入力して要求MACアドレスのテーブルエントリおよび要求MACアドレスのすべてのエントリを表示することもできます。

Syntax
show mac-addr-table [{<macaddr> < vlanid >|all}]

<macaddr> - MACアドレスを入力して要求MACアドレスのテーブルエントリを表示します。

<vlanid> - VLAN ID (範囲：1～4094)

all – このコマンドによりテーブル全体を表示します。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

MAC Address:

スイッチが転送またはフィルタリング情報を持つユニキャストのMACアドレス。形式はコロンで区切られた 6 個～8 個の 2 桁の 16 進数です。例えば、01:23:45:67:89:AB IVLシステムではMACアドレスは 8 バイトで表示されます。SVLシステムではMACアドレスは 6 バイトで表示されます。



このソフトウェアのバージョンはIVLシステムのみをサポートします。

Interface： L2 MACアドレスが学習されたポート

if Index: このポートに関連するインタフェイステーブルエントリのインターフェイス番号を示します。

ステータス： エントリのステータス。

値の内容は以下のとおりです。

Static – 静的MACフィルタが定義された際、システムまたはユーザーにより追加された該当インスタンスの値

Learned - 受信トラフィックの送信元MACアドレスを確認し、学習した該当インスタンスの値

Management - 該当インスタンスの値 (システムMACアドレス) は、 dot1dStaticAddress の既存インスタンスの値となります。この値はインタフェイス 3/1 と判断され、VLANを有効化しルーティングを行うために使用されます。

Self -対応するインスタンスの値はスイッチの物理インスタンス(システムの固有のMACアドレス)の 1 個のアドレスです。

GMRP Learned - 該当インスタンスの値をGMRP経由で学習し、マルチキャストに適用します。

Other - どのカテゴリにも分類されない該当インスタンスの値

9.4.2.2 show mac-addr-table count

このコマンドは合計の転送データベースエントリ、静的で習得中MACアドレスの数、及び、スイッチ上で利用できるアドレスの最大数を表示します。

Syntax
show mac-addr-table count

初期設定

なし

コマンド･モード

特権EXEC

表示メッセージ

Dynamic Address count: L2 MACアドレステーブルの取得MACアドレスの合計数

Static Address (User-defined) count: L2 MACアドレステーブルのユーザー定義アドレスの合計数

Total MAC Addresses in use: L2 MACアドレステーブルのアドレスの合計数

Total MAC Addresses available: スイッチはL2 MACアドレステーブルの最大値をサポートします。

9.4.2.3 **show mac-addr-table interface**

このコマンドにより転送データベースエントリを表示します。インタフェイス番号<slot/port>を使用し、FDBテーブルを検索できます。

Syntax
show mac-addr-table interface <slot/port>

<slot/port> - インタフェイス番号

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

MAC Address: スイッチが転送かつまたはフィルタリング情報を持つユニキャストのMACアドレス。 形式はコロンで区切られた 6 個～8 個の 2 桁の 16 進法の数字です。
例えば、01:23:45:67:89:AB IVLシステムではMACアドレスは 8 バイトで表示されます。
SVLシステムではMACアドレスは 6 バイトで表示されます。



このソフトウェアのバージョンはIVLシステムのみをサポートします。

注記:このソフトウェアバージョンはIVLシステムのみに対応しています。

VLAN ID: MACアドレスのVLAN ID

ステータス: エントリのステータス。

値の内容は以下のとおりです。

Static - 静的MACフィルタが定義された際、システムまたはユーザーにより追加された該当インスタンスの値

Learned - 受信トラフィックの送信元MACアドレスを確認し、学習した該当インスタンスの値 **Management -** 該当インスタンスの値 (システムMACアドレス) は、 dot1dStaticAddress の既存インスタンスの値となります。この値はインタフェイス 3/1 と判断され、VLANを有効化しルーティングを行うために使用されます。

Self -対応するインスタンスの値はスイッチの物理インスタンス(システムの固有のMACアドレス)の 1 個のアドレスです。

GMRP Learned :

対応するインスタンスの値はGMRP経由で習得され、マルチキャストに適用される。

Other - どのカテゴリにも分類されない該当インスタンスの値

9.4.2.4 **show mac-addr-table vlan**

このコマンドにより転送データベースエントリを表示します。VLAN IDによりFDBテーブルを検索できます。

Syntax
show mac-addr-table vlan <vlanid>

<vlanid> - VLAN ID (範囲： 1 – 4094)

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

MAC Address: スイッチが転送かつまたはフィルタリング情報を持つユニキャストのMACアドレス。 形式はコロンで区切られた 6 個～8 個の 2 桁の 16 進法の数字です。
例えば、01:23:45:67:89:AB IVLシステムではMACアドレスは 8 バイトで表示されます。
SVLシステムではMACアドレスは 6 バイトで表示されます。



このソフトウェアのバージョンはIVLシステムのみをサポートします。

注記：このソフトウェアバージョンはIVLシステムのみに対応しています。

インターフェイス： L2 MACアドレスが学習されたポート

ステータス： エントリのステータス。

値の内容は以下のとおりです。

Static - 静的MACフィルタが定義された際、システムまたはユーザーにより追加された該当インスタンスの値

Learned - 受信トラフィックの送信元MACアドレスを確認し、学習した該当インスタンスの値

Management - 該当インスタンスの値 (システムMACアドレス) は、 dot1dStaticAddress の既存インスタンスの値となります。この値はインタフェイス 3/1 と判断され、VLANを有効化しルーティングを行うために使用されます。

Self -対応するインスタンスの値はスイッチの物理インスタンス(システムの固有のMACアドレス)の 1 個のアドレスです。

GMRP Learned:対応するインスタンスの値はGMRP経由で習得され、マルチキャストに適用される。

Other - どのカテゴリにも分類されない該当インスタンスの値

9.4.2.5 show mac-address-table gmrp

このコマンドはマルチキャスト転送データベース(MFDB)テーブルのGARP(Generic Attributes Registration Protocol)のエントリを表示します。

Syntax
show mac-address-table gmrp

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Mac Address: スイッチが転送かつまたはフィルタリング情報を持つユニキャストのMACアドレス。 形式はコロンで区切られた 6 個～8 個の 2 桁の 16 進法の数字です。
例えば、01:23:45:67:89:AB　IVLシステムではMACアドレスは 8 バイトで表示されます。
SVLシステムではMACアドレスは 6 バイトで表示されます。



このソフトウェアのバージョンはIVLシステムのみをサポートします。

Type: これはエントリのタイプを表示します。静的エントリはエンドユーザーにより構成された項目です。動的エントリは習得過程やプロトコルの結果としてテーブルに追加されます。

Description: このマルチキャストテーブル・エントリの解説

Interfaces: 選択されたアドレスの転送(Fwd:)とフィルタリング(Flt:)に指定されたインターフェイスのリストです。

9.4.2.6 show mac-address-table igmpsnooping

このコマンドはマルチキャスト転送データベース(MFDB)テーブルのIGMPスヌーピングエントリを表示します。

Syntax
show mac-address-table igmpsnooping

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Mac Address: スイッチが転送かつまたはフィルタリング情報を持つユニキャストのMACアドレス。 形式はコロンで区切られた 6 個～8 個の 2 桁の 16 進法の数字です。
例えば、01:23:45:67:89:AB IVLシステムではMACアドレスは 8 バイトで表示されます。
SVLシステムではMACアドレスは 6 バイトで表示されます。



このソフトウェアのバージョンはIVLシステムのみをサポートします。

Type: これはエントリのタイプを表示します。静的エントリはエンドユーザーにより構成された項目です。動的エントリは習得過程やプロトコルの結果としてテーブルに追加されます。

Description: このマルチキャストテーブル・エントリの文章による解説

Interfaces: 選択されたアドレスの転送(Fwd:)とフィルタリング(Flt:)に指定されたインターフェイスのリストです。

9.4.2.7 show mac-address-table mldsnooping

このコマンドはマルチキャスト転送データベース(MFDB)テーブルのMLDスヌーピングのエントリを表示します。

Syntax
show mac-address-table mldsnooping

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Mac Address: スイッチが転送かつまたはフィルタリング情報を持つユニキャストのMACアドレス。 形式はコロンで区切られた 6 個～8 個の 2 桁の 16 進法の数字です。
例えば、01:23:45:67:89:AB IVLシステムではMACアドレスは 8 バイトで表示されます。
SVLシステムではMACアドレスは 6 バイトで表示されます。



このソフトウェアバージョンはIVLシステムのみに対応しています。

Type – これはエントリのタイプです。静的なエントリはエンドユーザーによって構成されるものです。 動的な項目は習得の手順やプロトコルの結果としてテーブルに追加されます。

Description – このマルチキャストテーブル・エントリを文章で解説したものです。

Interfaces: 選択されたアドレスの転送とフィルタリングに指定されたインターフェイスのリストです。

9.4.2.8 show mac-address-table multicast

このコマンドによりMFDB情報を表示します。パラメータをつけずにコマンドを入力するとテーブル全体が表示されます。*all*パラメータを入力した場合も同様です。任意のパラメータでMACアドレスを指定して、1 つのMACアドレスのテーブルエントリを表示できます。

Syntax
show mac-address-table multicast {<macaddr> <vlanid> | all }

<macaddr> - MACアドレスを入力して要求MACアドレスのテーブルエントリを表示します。

<vlanid> - VLAN ID (範囲:1～4094)

all – このコマンドによりテーブル全体を表示します。

初期設定

None

コマンド・モード

特権EXEC

表示メッセージ

Mac Address: スイッチが転送またはフィルタリング情報を持つユニキャストのMACアドレス。 形式はコロンで区切られた 6 個～8 個の 2 桁の 16 進数です。
例えば、01:23:45:67:89:AB IVLシステムではMACアドレスは 8 バイトで表示されます。
SVLシステムではMACアドレスは 6 バイトで表示されます。



このソフトウェアのバージョンはIVLシステムのみをサポートします。

Type: これはエントリのタイプを表示します。静的エントリはエンドユーザーにより構成された項目です。動的エントリは習得過程やプロトコルの結果としてテーブルに追加されます。

Source:マルチキャスト転送データベースでこのエントリに対応するコンポーネント。値は、IGMP Snooping、GMRP、およびStatic Filteringとなります。

Description: マルチキャストテーブルエントリのテキスト記述

Interfaces: 転送 (Fwd:) およびフィルタリング (Flt:) に指定されているインタフェイスのリスト

Forwarding Interfaces: すべてのコンポーネントの転送インターフェイスを結合し、静的フィルタリングインタフェイスとして列記されたインタフェイスを削除し、結果転送リストが作成されます。

9.4.2.9 **show mac-address-table stats**

このコマンドによりMFDB統計データを表示します。

Syntax
show mac-address-table stats

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Max MFDB Table Entries: MFDBにあるエントリの合計数を示します。

Most MFDB Entries Since Last Reset: マルチキャスト転送データベーステーブルにあったエントリの最大数を示します。この値はMFDBのピーク値といいます。

Current Entries: マルチキャスト転送データベーステーブルの現在のエントリ数を示します。

9.4.2.10 **show mac-addr-table agetime**

このコマンドにより転送データベースのアドレスエイジングタイムアウトを表示します。

Syntax
show mac-addr-table agetime

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Address Aging Timeout: 転送データベーステーブルの合計秒数を示します。

9.4.2.11 **mac-addr-table aging-time**

このコマンドにより転送データベースのアドレスエイジングタイムアウトを秒単位で設定します。

Syntax
mac-addr-table aging-time <10-1000000> no mac-addr-table aging-time <10-1000000>

<10-1000000> - エイジングタイム、秒単位 (範囲：10～1000000)

no - 転送データベースのアドレスエイジングタイムアウトを 300 秒に設定します。

初期設定

300

コマンド・モード

グローバル・コンフィグ

9.4.3 VLAN 管理

9.4.3.1 show vlan

このコマンドは構成されたすべてのVLANの簡略な情報を表示します。

Syntax
show vlan

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

VLAN ID: 各VLANに関連付けられたVLAN識別子(VID)があります。VLAN IDの範囲は 1 から 4094 です。

VLAN Name: このVLANへ便宜的に関連付けられた文字列です。ブランクを含め、32 字までの英数字が使えます。デフォルトはブランクです。VLAN ID 1 は常に「デフォルト」と名付けられます。この欄はオプションです。

VLAN Type: デフォルトになれるVLANのタイプ。(VLAN ID = 1) は静的(構成され恒久的に定義される)または、動的(GVRP登録で作成される)か可能です。

Interface(s): スロットIDとポート番号でどのポートがこのVLANに所属するのかを表示します。

9.4.3.2 show vlan id

このコマンドはインターフェイスの情報を含め、特定のVLANのための詳しい情報を表示します。

Syntax
show vlan {id <vlanid> | name <vlanname>}

<vlanid> - VLAN ID (範囲 1 から 4094)

<vlanname> - VLANの名前 (32 文字までの英数字)

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

VLAN ID: 各VLANに関連付けられたVLAN識別子(VID)があります。VLAN IDの範囲は 1 から 4094 です。

VLAN Name: このVLANへ便宜的に関連付けられた文字列です。 ブランクを含め、32 字までの英数字が使えます。デフォルトはブランクです。 VLAN ID 1 は常に「デフォルト」と名付けられます。この欄はオプションです。

VLAN Type: デフォルトになれるVLANのタイプ。(VLAN ID = 1) は静的(構成され恒久的に定義される)または、動的(GVRP登録で作成される)か可能です。

Interface : スロットIDとポート番号でどのポートがこのVLANに所属するのかを表示します。

最上部のセレクターによりすべてのポートのパラメータを設定できます。

Current: このVLANへこのポートが参加するレベルを決定する。許可される値は:

Include: このポートは常にこのVLANのメンバーです。 これはIEEE 802.1Q基準で修正された登録に等しい

Exclude: このポートは決してこのVLANのメンバーになり得ない。 これはIEEE 802.1Q基準で禁じられている登録に等しい。

Autodetect: GVRP経由でこのVLANへポートが動的に登録されるように特定する。参加の要求がこのポートで受信されなければポートはこのVLANへは参加しない。これはIEEE 802.1Q基準に正常に登録されているものに等しい。

Configured: このポートがこのVLANへ参加する構成された度合いを決定する。許可される値は:

Include: このポートは常にこのVLANのメンバーです。 これはIEEE 802.1Q規格に規定された登録内容と同じです。

Exclude – このポートは決してこのVLANのメンバーではありません。これはIEEE 802.1Q規格で禁止された登録内容と同じです。

Autodetect: GVRP経由でこのVLANへポートが動的に登録されるように指定する。参加の要求がこのポートで受信されなければポートはこのVLANへは参加しない。これはIEEE 802.1Q基準に正常に登録されているものに等しい。

Tagging: このVLANのこのポートへタグ付けする動作を選択する。

Tagged – このVLANへのトラフィックをタグ付けしたフレームとして送信するよう指定します。

Untagged – このVLANへのトラフックをタグ無しフレームとして送信するよう指定します。

9.4.3.3 show vlan association mac

このコマンドは特定の構成されたMACアドレスと関連付けられたVLANを表示します。MACアドレスが特定されなければ、構成されたMACアドレスのVLAN関連が表示されます。

Syntax
show vlan association mac [<macaddr>]

<macaddr> - 要求されたMACアドレスに対しテーブル・エントリを表示するためMACアドレスを入力する。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Mac Address: スイッチが転送またはフィルタリング情報を持つユニキャストのMACアドレス。 形式はコロンで区切られた 6 個～8 個の 2 桁の 16 進数です。
例えば、01:23:45:67:89:AB IVLシステムではMACアドレスは 8 バイトで表示されます。
SVLシステムではMACアドレスは 6 バイトで表示されます。.



このソフトウェアのバージョンはIVLシステムのみをサポートします。

VLAN ID: 各VLANに関連付けられたVLAN識別子(VID)があります。VLAN IDの範囲は 1 から 4094 です。

9.4.3.4 show vlan association subnet

このコマンドは特定の構成されたIPアドレスとネットマスクに関連付けされたVLANを表示します。 IPアドレスとネットマスクが指定されない場合、すべての構成されたIPサブネットのVLAN関連が表示されます。

Syntax
show vlan association subnet [<ipaddr> <netmask>]

<ipaddr> - IPアドレス

<netmask> - サブネットマスク

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

IP Address: インターフェイス毎に割当てられるIPアドレス

IP Mask: サブネットマスク

VLAN ID: 各VLANに関連付けられたVLAN識別子(VID)があります。VLAN IDの範囲は 1 から 4094 です。

9.4.3.5 **show protocol group**

このコマンドはシステム全体または表示されたグループのためのプロトコルベースのVLAN情報を表示します。

Syntax
show protocol group {<group-name> | all}

<group-name> - プロトコルベースのVLANテーブルにあるエントリのグループ名.

すべて – テーブル全体を表示します。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Group Name : この欄はプロトコルベースのVLANテーブルの中のエントリのグループ名を表示します。

Group ID: この欄はプロトコルグループのグループ識別子を表示します。

Protocol(s): この欄はこのグループのプロトコルのタイプを表示します。

VLAN: この欄はこのプロトコルグループに関連付けられたVLANを表示します。

Interface(s): この欄はこのプロトコルグループに関連付けられたスロットまたはポートインターフェイスをリストします。

9.4.3.6 **show interface switchport**

このコマンドはVLANポート情報を表示する。

Syntax
show interface switchport {<slot/port> | all}

<slot/port> - インターフェイス番号

all – テーブル全体を表示する

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Interface: スロットIDとポート番号でどのポートがこのラインの欄により制御されているのかを表示します。 最上部のセレクターによりすべてのポートのパラメータを設定できます。

Port VLAN ID: このポートで受信されたタグ無しのフレームまたはプライオリティタグ付きのフレームをこのポートが割当てるVLAN IDです。値は存在するVLANでなければなりません 。工場出荷時デフォルトは 1 です。

Acceptable Frame Types: このポートで受信できるフレームのタイプを指定します。オプションは「VLANのみ」と「すべて許可」です。「VLANのみ」に設定するとこのポートで受信するタグ無しフレームかプライオリティタグ付きフレームは破棄されます。「すべて許可」に設定されるとこのポートで受信されるタグ無しフレームまたはプライオリティタグ付きのフレームは許可され、このポートのポートVLAN IDの値が割当てられます。いずれのオプションでも、VLANタグ付きのフレームは 802.1Q VLAN規格に従って転送されます。
Ingress Filtering: 有効化または無効化できます。有効化されると、このポートがこのフレームが関連付けられたVLANのメンバーでなければフレームは破棄されます。タグ付きのフレームではVLANはタグ中のVLAN IDで識別されます。タグ無しのフレームではVLANはこのフレームを受信したポートに指定されたポートVLAN IDです。無効化されている場合すべてのフレームは 802.1Qブリッジ規格に従って転送されます。工場出荷時デフォルトは無効化です。

GVRP: 有効化または無効化できます。

Default Priority: ポートに到着するタグ無しパケットに割当てられた 802.1pプライオリティに割当てられたプライオリティ。

9.4.3.7 VLAN database

このコマンドはVLANインターフェイス・コンフィグモードへ入力するために使われます。

Syntax
VLAN database

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.4.3.8 vlan

このコマンドは新しいVLANを作成し、それにIDを割当てます。 このIDは有効なVLAN識別番号です。(ID 1 はデフォルトVLANのため予約) VLANの範囲は 2 から 4094 です。

Syntax
vlan <vlanid> [<name>] no vlan <vlanid>

<vlanid> - VLAN ID (範囲 1 から 4094)

<name> - オプションのVLAN名を構成します(1 から 32 字の英数字)

no - このコマンドは既存のVLANを削除します。IDは有効なVLAN識別番号です(ID 1 はデフォルトVLANのため予約) VLANの範囲は 2 から 4094 です。

初期設定

なし

コマンド・モード

VLAN データベース

9.4.3.9 vlan name

このコマンドはVLANの名前を変更します。名前は 32 字までの英数字文字列です。IDは有効なVLAN識別番号です。IDの範囲は 1 から 4094 です。

Syntax
vlan name <vlanid> <newname> no vlan name <vlanid>

<vlanid> - VLAN ID(範囲は 1 から 4094)

<newname> - 新しいVLAN名を構成する。(32 字までの英数字)

no - このコマンドはVLAN名をデフォルト設定の文字列に設定します。VLAN IDは有効なVLAN識別番号です。IDの範囲は 1 から 4094 です。

初期設定

VLAN ID 1 の名前は常に“Default“という文字列です。他のVLANのデフォルト名 は VLAN0002 か らVLAN4094 の文字列です。

コマンド・モード

VLAN データベース

9.4.3.10 vlan association mac

このコマンドはMACアドレスをVLANへ関連付けます。

Syntax
vlan association mac <macaddr> <vlanid> no vlan association mac <macaddr>

<macaddr> - 要求されたMACアドレスのテーブル･エントリを表示するために入力する

<vlandid> - VLAN識別番号。 IDの範囲は 1 から 4094 です。

no – このコマンドはMACアドレスのVLANへの関連付けを削除します。

初期設定

なし

コマンド･モード

VLAN データベース

9.4.3.11 vlan association subnet

このコマンドはIPサブネットをVLANに関連付けます。

Syntax
vlan association subnet <ipaddr> <netmask> <vlanid> no vlan association subnet <ipaddr> <netmask>

<ipaddr> - IPアドレス

<netmask> - サブネットマスク

<vlandid> - VLAN識別番号。IDの範囲 1 から 4094

no - このコマンドは特定のIPサブネットのVLANへの関連付けを削除します。

初期設定

None

コマンド･モード

VLAN データベース

9.4.3.12 vlan makestatic

このコマンドは動的に作成されたVLAN(GVRP登録で作成されたもの)を静的なVLAN(恒久的に構成され定義されたもの)へ変換します。IDは有効な識別番号です。VLANの範囲は 2 から 4094 です。

Syntax
vlan makestatic <vlanid>

<vlanid> - VLAN ID (Range: 2 –4094).

初期設定

なし

コマンド・モード

VLAN データベース

9.4.3.13 protocol group

このコマンドは<vlanid>を<group-name>で識別されたプロトコルベースのVLANへ付けます。ひとつのグループは一度にひとつのVLANのみ関連付けできます、しかしながらVLANの関連付けは変更可能です。

Syntax
protocol group <group-name> <vlanid> no protocol group <group-name> <vlanid>

<vlanid> - VLAN ID(範囲は 1 から 4094)

<group-name> - VLANグループ名(1 から 16 文字の文字列)

no - このコマンドはこの<group-name>によって識別されるプロトコルベースのVLANグループから<vlanid>を削除します。

初期設定

None

コマンド・モード

VLAN データベース

9.4.3.14 **switchport acceptable-frame-type**

このコマンドはインターフェイス毎にフレーム承認モードを設定します。VLANのみのモードでは、このインターフェイス上で受信されたタグ無しフレームまたはプライオリティフレームは破棄されます。すべて許可モードでは、このインターフェイスで受信されたタグ無しフレームまたはプライオリティフレームは許可され、このポートへのインターフェイスVLAN IDの値を割当てられます。。いずれのオプションでも、VLANタグ付きフレームはIEEE 802.1Q VLAN規格に従って転送されます。

Syntax
switchport acceptable-frame-type {tagged | all} no switchport acceptable-frame-type {tagged | all}

Tagged – **VLANのみのモード**

all – **すべて許可モード**

no - このコマンドはインターフェイス毎のフレーム承認モードをすべて許可に設定します。すべて許可モードでは、このインターフェイス上で受信されたタグ無しフレームまたはプライオリティフレームは許可され、このポートへのインターフェイスVLAN IDの値を割当てられます。いずれのオプションでも、VLANタグ付きフレームはIEEE 802.1Q VLAN規格に従って転送されます。

初期設定

すべて許可

コマンド・モード

インターフェイス・コンフィグ

このコマンドはフレーム承認モードをすべてのインターフェイスに設定します。VLANのみのモードでは、このインターフェイス上で受信されたタグ無しフレームまたはプライオリティフレームは破棄されます。 すべて許可モードでは、このインターフェイス上で受信されたタグ無しフレームまたはプライオリティフレームは許可され、このポートへのインターフェイスVLAN IDの値を割当てられます。いずれのオプションでも、VLANタグ付きフレームはIEEE 802.1Q VLAN規格に従って転送されます 。

Syntax
switchport acceptable-frame-type all {tagged | all} no switchport acceptable-frame-type all {tagged | all}

tagged – VLANのみのモード

all – 一つはすべて許可モードのため、もう一つはすべてのインターフェイスのためです。

no - このコマンドはすべてのインターフェイスのフレーム承認モードを**すべて許可**に設定します。すべて許可モードでは、このインターフェイス上で受信されたタグ無しフレームまたはプライオリティフレームは許可され、このポートへのインターフェイスVLAN IDの値を割当てられます。いずれのオプションでも、VLANタグ付きフレームはIEEE 802.1Q VLAN規格に従って転送されます。

初期設定

すべて許可

コマンド・モード

グローバル・コンフィグ

9.4.3.15 switchport ingress-filtering

このコマンドは入口フィルタリングを有効化します。入口フィルタリングが無効化されていると、インターフェイスを受信するVLANのメンバー資格に一致しないVLAN IDとともに受信されたフレームは許可されそのVLANのメンバーであるポートへ転送されます。

Syntax
switchport ingress-filtering no switchport ingress-filtering

no - このコマンドは入口フィルタリングを無効化します。入口フィルタリングが無効化されている場合、インターフェイスを受信するVLANのメンバー資格に一致しないVLAN IDとともに受信したフレームは許可されそのVLANのメンバーであるポートへ転送されます。

初期設定

無効

コマンド・モード

インターフェイス・コンフィグ

このコマンドは入口フィルタリングを有効化します。入口フィルタリングが無効化されている場合、インターフェイスを受信するVLANのメンバー資格に一致しないVLAN IDとともに受信したフレームは許可されそのVLANのメンバーであるポートへ転送されます。

Syntax
switchport ingress-filtering all no switchport ingress-filtering all

all – すべてのインターフェイス **no -** このコマンドは入口フィルタリングを無効化します。入口フィルタリングが無効化されている場合、インターフェイスを受信するVLANのメンバー資格に一致しないVLAN IDとともに受信したフレームは許可されそのVLANのメンバーであるポートへ転送されます。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

9.4.3.16 switchport native vlan

このコマンドはインターフェイス毎のVLAN IDを変更します。

Syntax
switchport native vlan <vlanid> no switchport native vlan <vlanid>

<vlanid> - VLAN ID(範囲は 1 から 4094)

no - このコマンドはインターフェイス毎のVLAN IDを 1 に設定します。

初期設定

1

コマンド・モード

インターフェイス・コンフィグ

このコマンドはすべてのインターフェイスのVLAN IDを変更します。

Syntax
switchport native vlan all <vlanid>

<vlanid> - VLAN ID(範囲は 1 から 4094)

all – すべてのインターフェイス

no - このコマンドはすべてのインターフェイスのVLAN IDを 1 に設定します。

初期設定

1

コマンド・モード

グローバル・コンフィグ

9.4.3.17 **switchport allowed vlan**

このコマンドはあるVLANの特定のインターフェイスのための参加のレベルを構成します。IDは有効な識別番号で、インターフェイスは有効なインターフェイス番号です 。

Syntax
switchport allowed vlan {add [tagged | untagged] | remove} <vlanid>

<vlanid> - VLAN ID(範囲は 1 から 4094)

add – インターフェイスは常にこのVLANのメンバーです。これは修正された登録に等しい。

tagged – このVLANへ送信されたすべてのフレームはタグ付けされます。

untagged – このVLANへ送信されたすべてのフレームはタグ付けされません。

remove – インターフェイスがこのVLANのメンバーから削除されます。これは禁止された登録に等しい。

初期設定

None

コマンド・モード

インターフェイス・コンフィグ

このコマンドはすべてのインターフェイスのVLANへの参加の度合いを構成します。IDは有効な識別番号です。

Syntax
switchport allowed vlan {add {tagged | untagged} | remove} all <vlanid>

<vlanid> - VLAN ID(範囲は 1 から 4094)

all – すべてのインターフェイス

add – インターフェイスは常にこのVLANのメンバーです。これは修正された登録に等しい。

tagged – このVLANへ送信されたすべてのフレームはタグ付けされます。
untagged – このVLANへ送信されたすべてのフレームはタグ付けされません。

remove – インターフェイスがこのVLANのメンバーから削除されます。これは禁止された登録に等しいです。

初期設定

None

コマンド・モード

グローバル・コンフィグ

9.4.3.18 switchport tagging

このコマンドはVLANの特定のインターフェイスのタグ付け動作を有効に構成します。タグ付けが有効化されていると、トラフィックはタグ付きのフレームとして送信されます。タグ付けが無効化された場合、トラフィックはタグ無しのフレームとして送信されます。IDは有効なVLAN識別番号です。

Syntax

```
switchport tagging <vlanid>
no switchport tagging <vlanid>
```

<vlanid> - VLAN ID(範囲は 1 から 4094)

no - このコマンドはVLANの特定インターフェイスのタグ付け動作を無効化します。タグ付けが無効化された場合、トラフィックはタグ無しのフレームとして送信されます。IDは有効なVLAN 識別番号です。

初期設定

Disabled

コマンド・モード

インターフェイス・コンフィグ

このコマンドはVLANの特定のインターフェイスのタグ付け動作を有効に構成します。タグ付けが有効化されていると、トラフィックはタグ付きのフレームとして送信されます。タグ付けが無効化された場合、トラフィックはタグ無しのフレームとして送信されます。IDは有効なVLAN識別番号です。

Syntax

```
switchport tagging all <vlanid>
```

<vlanid> - VLAN ID(範囲は 1 から 4094)

すべて – すべてのインターフェイス

no - このコマンドはVLANの特定のインターフェイスのタグ付け動作を無効化します。タグ付けが無効化された場合、トラフィックはタグ無しのフレームとして送信されます。IDは有効なVLAN 識別番号です。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

9.4.3.19 **switchport priority**

このコマンドはタグ無しパケットに割当てられたデフォルトの 802.1pポートプライオリティを特定のインターフェイスのために構成します。

Syntax
switchport priority <0-7>

<0-7> - プライオリティの範囲は 0-7 です。

初期設定

0

コマンド・モード

インターフェイス・コンフィグ

このコマンドはデバイスに現在接続されているすべてのポートにおいてタグ無しパケットに割当てられたポートプライオリティを構成します。その結果ポート毎の構成はこの構成を上書きします。

Syntax
switchport priority all <0-7>

<0-7> - プライオリティの範囲は 0 から 7

すべて – すべてのインターフェイス

初期設定

0

コマンド・モード

グローバル・コンフィグ

9.4.3.20 **switchport protocol group**

このコマンドは物理<slot/port>インターフェイスをグループ名によって識別されるプロトコルベースのVLANへ追加します。グループはそれに関連付けられたインターフェイスを 1 個以上持つことがあります。各インターフェイスとプロトコルの組み合わせはひとつのグループのみ関連付けられます。グループへインターフェイスを追加するグループに現在関連付けられているプロトコルと競合する場合、このコマンドは失敗しインターフェイスはグループに追加されません 。

Syntax
switchport protocol group <group-name> no switchport protocol group <group-name>

<group-name> - VLANグループ名(1 から 16 文字の文字列)

no - このコマンドはこの*<group-name>*に識別されるプロトコルベースのVLANグループからインターフェイスを削除します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

このコマンドはシステムにプロトコルベースのVLANグループを追加します。*<group-name>*は 1～16 文字の文字列です。作成されると、そのプロトコルグループは後に来るコマンドでグループを識別するための固有番号を割当てられます。

Syntax
switchport protocol group <group-name> no switchport protocol group <group-name>

<group-name> - VLANグループ名(1 から 16 文字の文字列)

no - このコマンドはこの<group-name>によって識別されるプロトコルベースのVLANを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドはすべての物理インターフェイスを<group-name>で識別されたプロトコルベースのVLANへ追加します。グループはそれに関連付けられたインターフェイスを一つ以上持つことがあります。各インターフェイスとプロトコルの組み合わせは 1 個のグループのみ関連付けられます。グループへインターフェイスを追加するグループに現在関連付けられているプロトコルと競合する場合、このコマンドは失敗しインターフェイスはグループに追加されません 。

Syntax
switchport protocol group all <group-name> no switchport protocol group all <group-name>

<group-name> - VLANグループ名(1 から 16 文字の文字列)

all – すべてのインターフェイス no - このコマンドはこの<group-name>によって識別されるこのプロトコルベースのVLANグループからすべてのインターフェイスを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドは<group-name>により識別されたプロトコルベースのVLANへ<protocol>を追加します。グループはそれに関連付けられたインターフェイスを一つ以上持つことがあります。各インターフェイスとプロトコルの組み合わせは 1 個のグループのみと関連付けられます。グループへインターフェイスを追加するグループに関連付けられているプロトコルと競合する場合、このコマンドは失敗しインターフェイスはグループに追加されません。プロトコルに可能な値は、ip、arp、ipxです 。

Syntax
switchport protocol group add protocol <group-name> {ip | arp | ipx} no switchport protocol group add protocol <group-name> {ip | arp | ipx}

<group-name> - VLANグループ名(1 から 16 文字の文字列)

ip - IPプロトコル

arp - ARPプロトコル

ipx - IPXプロトコル

no - このコマンドは<group-name>により識別されたプロトコルベースのVLANへ<protocol>を追加します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.4.3.21 switchport forbidden vlan

このコマンドは禁止されたVLANを構成する際使用します。

Syntax
switchport forbidden vlan {add | remove} <vlanid> no switchport forbidden

<vlanid> - VLAN ID(範囲は 1 から 4094)

add –VLAN IDを追加

remove –VLAN IDを削除

no -禁止されたVLANのリストを削除する

初期設定

なし

コマンド･モード

インターフェイス･コンフィグ

9.4.4 GVRP and Bridge Extension (GVRP とブリッジ拡張)

9.4.4.1 show bridge-ext

このコマンドによりGARP情報を表示します。

Syntax
show bridge-ext

初期設定

None

コマンド・モード

特権EXEC

表示メッセージ

GMRP Admin Mode: これはシステムのGARPマルチキャスト登録プロトコルの管理モードを表示します。

GVRP Admin Mode: これはシステムのGARP VLAN登録プロトコル(GVRP)の管理モードを表示します。

9.4.4.2 show gvrp configuration

このコマンドは 1 個またはすべてのインターフェイスのGARP (Generic Attributes Registration Protocol) 情報を表示します。

Syntax
show gvrp configuration {<slot/port> | all}

<slot/port> - An インターフェイス番号

すべて – すべてのインターフェイス

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Interface: 説明するインターフェイスのスロット/ポートを表示します 。

Join Timer: GARP PDUがある属性のためのメンバー資格を登録(または再登録)する送信の間隔を指定します。現在の属性はVLANまたはマルチキャストグループです。このタイマーにはポート毎、GARP毎に参加するベースのインスタンスがあります。許可される値は 10 から 100 センチ秒(0.1～1.0 秒)です。工場出荷時デフォルトは 20 センチ秒(0.2 秒)です。規格の最高の精度は 1 センチ秒(0.01 秒)です。

Leave: 属性の登録を解除する要求を受信した後、その属性を削除するまでに待機する時間を指定します。現在の属性はVLANまたはマルチキャストグループです。これは中断しないサービスを維持するため他のステーションがこれと同じ属性の登録を強制するバッファー時間と見ることができます。ポート毎、GARP毎に参加するインスタンスがこのタイマーにあります。許可される値は 20～600 センチ秒(0.2～6.0 秒)です。工場出荷時デフォルトは 60 センチ秒(0.6 秒)です。規格の最高精度は 1 センチ秒(0.01 秒)です。

LeaveAll : LeaveAll TimeはLeaveAll PDU間隔を制御します。LeaveAll PDUはすべての登録がまもなく抹消されることを示します。参加者は登録を維持するためには再参加する必要があります。ポート毎、GARP毎に参加するベースのインスタンスがこのタイマーにあります。 LeaveAll期間タイマーはLeaveall時間からLeaveall時間の 1.5 倍までのランダムな値に設定されます。許可される値は 200～6000 センチ秒(2～60 秒)です。工場出荷時デフォルトは 1000 センチ秒(10 秒)です。規格の最高精度は 1 センチ秒(0.01 秒)です 。

ポートGVRPモード: これはポートのGVRP管理モードを示します。有効化または無効化できます。このパラメータが無効化されると、Join Time、Leave Time、とLeave All Timeは効果がありません。工場出荷時デフォルトは無効化です。

9.4.4.3 show gmrp configuration

このコマンドは 1 個またはすべてのインターフェイスのGARP (Generic Attributes Registration Protocol) 情報を表示します。

Syntax
show gmrp configuration {<slot/port> | all}

<slot/port> - インターフェイス番号

all – すべてのインターフェイス

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Interface: これはテーブルのこの行が解説するインターフェイスのスロット/ポートを表示します。

Join Timer: GARP PDUがある属性のためのメンバー資格を登録(または再登録)する送 信の間 隔を指定します。現在の属性はVLANまたはマルチキャストグループです。このタイマーにはポート毎、GARP毎に参加するベースのインスタンスがあります。許可される値は 10 から 100 センチ秒(0.1～1.0 秒)です。工場出荷時デフォルトは 20 センチ秒(0.2 秒)です。規格の最高の精度は 1 センチ秒(0.01 秒)です。

Leave Timer: 属性の登録を解除する要求を受信した後、その属性を削除するまで に待機す る時間を指定します。現在の属性はVLANまたはマルチキャストグループです。これは中断しないサービスを維持するため他のステーションがこれと同じ属性の登録を強制するバッファー時間と見ることができます。ポート毎、GARP毎に参加するインスタンスがこのタイマーにあります。許可される値は 20～600 センチ秒(0.2～6.0 秒)です。工場出荷時デフォルトは 60 センチ秒(0.6 秒)です。規格の最高精度は 1 センチ秒(0.01 秒)です。

LeaveAll Timer: このLeaveAll Timeはどのくらい頻繁にLeaveAll PDUが作成さ れるかを制御します。LeaveAll PDUはすべての登録がまもなく登録抹消されることを示します。 参加者は登録 を維持するためには再参加する必要があります。ポート毎、GARP毎に参加するベースのインスタンスがこのタイマーにあります。LeaveAll期間タイマーはLeaveall時間からLeaveall時間の 1.5 倍までのランダムな値に設定されます。許可される値は 200～6000 センチ秒(2～60 秒)です。工場出荷時デフォルトは 1000 センチ秒(10 秒)です。規格の最高精度は 1 センチ秒(0.01 秒)です。

Port GMRP Mode: これはポートのGVRP管理モードを示します。有効化または無効化できます。このパラメータが無効化されると、Join Time、Leave Time、とLeave All Timeは効果がありません。工場出荷時デフォルトは無効化です。

9.4.4.4 show garp configuration

This command displays GMRP and GVRP configuration information for one or all interfaces.

Syntax
show garp configuration {<slot/port> | all}

<slot/port> - インターフェイス番号

all – すべてのインターフェイス

初期設定

None

コマンド・モード

特権EXEC

表示メッセージ

Interface: これはテーブルのこの行が解説するインターフェイスのスロット/ポートを表示します。

GVRPモード: これはポートのGVRP管理モードを示します。 有効化または無効化できます。 このパラメータが無効化されると、Join Time、Leave Time、とLeave All Timeは効果がありません。工場出荷時デフォルトは無効化です。

GMRPモード: これはポートのGMRP管理モードを示します。有効化または無効化できます。 このパラメータが無効化されると、Join Time、Leave Time、とLeave All Timeは効果がありません 。工場出荷時 デフォルトは無効化 です。

9.4.4.5 **bridge-ext gvrp**

このコマンドはGVRPを有効化します。デフォルトは無効化です。

Syntax
bridge-ext gvrp no bridge-ext gvrp

no - このコマンドはGVRPを無効化します。



GVRP can't be 有効化 as the VTP function is 有効化.

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

9.4.4.6 **bridge-ext gmrp**

このコマンドはそのシステムのGARP(Generic Attributes Registration Protocol)を有効化します。デフォルトは無効化です。

Syntax
bridge-ext gmrp no bridge-ext gmrp

no - このコマンドはそのシステムのGARP(Generic Attributes Registration Protocol)を無効化します。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

9.4.4.7 switchport gvrp

このコマンドは特定のポートのGVRP (GARP VLAN Registration Protocol)を有効化します。

Syntax
switchport gvrp no switchport gvrp

no - このコマンドは特定のポートのGVRP (GARP VLAN Registration Protocol)を無効化します。GVRPが無効化されている場合Join Time、Leave Time、とLeave All Timeは効果がありません。

初期設定

Disabled

コマンド・モード

インターフェイス・コンフィグ

このコマンドはすべてのポートのGVRP (GARP VLAN Registration Protocol)を有効化します。

Syntax
switchport gvrp all no switchport gvrp all

all – すべてのインターフェイス

no - このコマンドはすべてのポートのGVRP (GARP VLAN Registration Protocol)を無効化します。GVRPが無効化されている場合Join Time、Leave Time、とLeave All Timeは効果がありません。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

9.4.4.8 **switchport gmrp**

このコマンドは選択されたインターフェイスのGMRPマルチキャスト登録プロトコルを有効化します。GMRPが有効のインターフェイスがルーティングを有効化した場合やポートチャンネル(LAG)のメンバーとして記載されている場合、GMRPの機能はそのインターフェイスでは無効化されます。GMRPの機能はその後ルーティングが無効化された場合やポートチャンネル(LAG)メンバー資格がGMRPが有効なインターフェイスから削除されたりすると再度有効化されます。

Syntax
switchport gmrp no switchport gmrp

no - **このコマンドは選択されたインターフェイスのGMRPマルチキャスト登録プ ロトコルを無効化します。GMRPが有効のインターフェイスがルーティングを有効化した場合やポートチャンネル(LAG)のメンバーとして記載されている場合、GMRPの機能性はそのインターフェイスでは無効化されます。GMRPの機能性はその後にルーティングが無効化された場合やポートチャンネル(LAG)メンバー資格がGMRPが有効なインターフェイスから削除されると再度有効化されます。**

初期設定

Disabled

コマンド・モード

インターフェイス・コンフィグ

このコマンドはすべてのインターフェイスのGMRPマルチキャスト登録プロトコルを有効化します。GMRPが有効のインターフェイスがルーティングを有効化した場合やポートチャンネル(LAG)のメンバーとして記載されている場合、GMRPの機能性はそのインターフェイスでは無効化されます。GMRPの機能性はその後にルーティングが無効化された場合やポートチャンネル(LAG)メンバー資格がGMRPが有効なインターフェイスから削除されると再度有効化されます。

Syntax
switchport gmrp all no switchport gmrp all

all – すべてのインターフェイス

no - このコマンドは選択されたインターフェイスのGMRPマルチキャスト登録プロトコルを無効化します。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

9.4.4.9 garp timer

このコマンドはGVRPのポート毎、GARP毎にGVRPjoin timeを設定します。Join TimeはGARPプロトコルデータユニット(PDU)がVLANまたはマルチキャストグループへ登録(または再登録)される時間間隔です。

このコマンドはGVRPとGMRPが有効化されている場合効果があります。時間は 10～100(センチ秒)です。

Syntax
garp timer join <10-100> no garp timer join

<10-100> - join time (範囲 10～100)センチ秒です。

no - このコマンドはポート毎そしてGARP毎のGVRPのjoin timeを 20 センチ秒(0.2 秒)に設定します。このコマンドはGVRPとGMRPが有効なときのみ効果があります。



このコマンドはGVRPまたはGMRPが有効なときのみ効果があります。

初期設定

20 センチ秒(0.2 秒)

コマンド・モード

インターフェイス・コンフィグ

このコマンドはGVRPのポート毎、GARP毎のGVRPjoin timeを設定します。Join TimeはGARPプロトコルデータユニット(PDU)がVLANまたはマルチキャストグループへ登録(または再登録)する送信時間間隔です。

このコマンドはGVRPとGMRPが有効化されている場合効果があります。時間は 10～100(センチ秒)です。

Syntax
garp timer join all < 10-100 > no garp timer join all

<10-100> - join time(範囲 10～100)センチ秒

all – すべてのインターフェイス

no - このコマンドはすべてのポートそしてGARP毎のGVRPのjoin timeを 20 センチ秒(0.2 秒)に設定します。このコマンドはGVRPとGMRPが有効なときのみ効果があります。


このコマンドはGVRPまたはGMRPが有効なときのみ効果があります。

初期設定

20 センチ秒(0.2 秒)

コマンド・モード

グローバル・コンフィグ

このコマンドはポート毎のGVRP leave timeを設定します。 Leave timeはVLANまたはマルチキャストグループへの登録抹消の要求を受信後、VLANエントリを削除するまで待機時間です。これはサービスを中断せず維持するために別のステーションがそれと同じ属性の登録を強制するためのバッファー時間です。時間は 20～600 センチ秒です 。

Syntax

```
garp timer leave < 20-600 >
no garp timer leave
```

<20-600> - leave time (範囲 20～600)センチ秒

no - このコマンドはGVRPのポート毎のleave timeを 60 センチ秒(0.6 秒)に設定します。



このコマンドはGVRPまたはGMRPが有効な場合のみ効果を発揮します。

初期設定

60 センチ秒(0.6 秒)

コマンド・モード

インターフェイス・コンフィグ

このコマンドはすべてのポートのGVRPのleave timeを設定します。Leave timeはVLANまたはマルチキャストグループへの登録抹消の要求を受信後、VLANエントリを削除するまでに待機する時間です。これはサービスを中断せず維持するために別のステーションがそれと同じ属性の登録を強制するためのバッファー時間としてとらえられます。時間は 20～600 センチ秒です。

Syntax
garp timer leave all < 20-600 > no garp timer leave all

<20-600> - Leave time (範囲 20～600)センチ秒

all – **すべてのインターフェイス**

no - **このコマンドはGVRPのポート毎のleave timeを 60 センチ秒(0.6 秒)に設定します。**



このコマンドはGVRPまたはGMRPが有効な場合のみ効果を発揮します。

初期設定

60 センチ秒 (0.6 秒) **コマンド・モード**

グローバル・コンフィグ

このコマンドはポート毎にLeaveAll PDUを作成する頻度を制御します。LeaveAll PDUはすべての登録が登録抹消されることを示します。参加者は登録を維持するためには再参加する必要があります。値はポート毎そしてGARP毎に適用されます。時間は 200～6000 センチ秒(2～60 秒)です。

Syntax

```
garp timer leaveall < 200-6000 >
no garp timer leaveall
```

<200-6000> - leave time (範囲 200～6000)センチ秒

no - このコマンドはポート毎に作成されるLeave All PDUの作成頻度を 1000 センチ秒(10 秒)に設定します。



このコマンドはGVRPまたはGMRPが有効な場合のみ効果を発揮します。

初期設定

1000 センチ秒(10 秒)

コマンド･モード

インターフェイス･コンフィグ

このコマンドはすべてのポートにLeaveAll PDUが割合で作成されるかを制御します。LeaveAll PDUはすべての登録が抹消されることを示します。参加者は登録を維持するためには再参加する必要があります。値はポート毎、GARP毎に適用されます。時間は 200～6000 センチ秒(2～60 秒)です 。

Syntax
garp timer leaveall all < 200-6000 > no garp timer leaveall all

<200-6000> - leave time (範囲 200～6000)センチ秒

all – すべてのインターフェイス

no - このコマンドはすべてのポートで作成されるLeave All PDUの作成頻度を 1000 センチ秒(10 秒)に設定します。



このコマンドはGVRPまたはGMRPが有効な場合のみ効果を発揮します。

初期設定

1000 センチ秒 (10 秒)コマンド・モード

グローバル・コンフィグ

9.4.5 VTP Commands (VTP コマンド)

9.4.5.1 show vtp counters

このコマンドはVTPパケットの統計を表示します、VTPの通知の送受信とVTPのエラーも含まれます。

Syntax
show vtp counters

初期設定

None

コマンド・モード

特権EXEC

表示メッセージ

Summary advertisements received: トランクポートでこのスイッチにより受信したサマリ通知の数。

Subset advertisements received: トランクポートでこのスイッチにより受信した通知のサブセットの数。

Request advertisements received: トランクポートでこのスイッチにより受信した通知の要求の数。

Summary advertisements transmitted: トランクポートでこのスイッチで送信されたサマリ通知の数。

Subset advertisements transmitted: トランクポートでこのスイッチで送信された通知のサブセットの数。

Request advertisements transmitted: トランクポートでこのスイッチで送信された通知の要求の数。

Number of config revision errors: 改訂エラーの数。

Number of config digest errors: MD5 ダイジェスト・エラーの数。

9.4.5.2 show vtp password

このコマンドはVTPドメインのパスワードを表示します。

Syntax
show vtp password

初期設定

None

コマンド・モード

特権EXEC

表示メッセージ

VTP Password: VTPドメインパスワードの表示

9.4.5.3 show vtp status

このコマンドはVTPドメインのステータスを表示します。

Syntax
show vtp status

初期設定

None

コマンド・モード

特権EXEC

表示メッセージ

VTP Status: VTPが有効化されているか無効化されているかを表示します。

VTP Version: スイッチで稼働するVTPのバージョンを表示します。

Configuration Revision: スイッチ上の現在の構成改訂番号

Maximum VTP supported VLANs: ローカルでサポート されたVLANの最大限数

VTP support VLAN number: 現在のVLANの数

VTP Operating Mode: VTPが稼働するモードを表示します。サ ーバ、クライア ントまたはトランスペアレント 3 モードが可能です 。

VTP Domain Name: スイッチの管理ドメインを識別する名前。

VTP Pruning Mode: プルーニングが有効化されているか無効化さ れているかを表示します。

MD5 digest: VTPドメイン・ステータスのチェックサム値を表示します。

Configuration last modified: 最後に構成が変更された日付と時間を表示します。構成の変更をデータベースに反映させたスイッチのIPアドレスを表示します。

9.4.5.4 show vtp trunkport

このコマンドはVTPトランクポートのステータスを表示します。

Syntax
show vtp trunkport

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Port: インターフェイス番号を表示します

Trunkport: インターフェイス番号のトランクポートステータス(有効化か無効化)を表示します。

9.4.5.5 **vtp**

このコマンドはグローバルVTP管理モードを構成するために使います。

Syntax
vtp no vtp

no - このコマンドはグローバルVTP管理モードを無効化します。

初期設定

有効化

コマンド･モード

グローバル･コンフィグ

9.4.5.6 **vtp domain**

このコマンドはVTP管理ドメイン名を設定するために使います。

Syntax
vtp domain <string> no vtp domain

<string> - ドメイン名の文字列を構成します(最大長 32 バイト)

no - このコマンドはドメイン名をなしにリセットします。

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.4.5.7 vtp mode

このコマンドはVTPデバイスモードを設定するために使います。クライアント、サーバ、トランスペアレントの 3 つのモードで構成できます。

Syntax
vtp mode { client | server | transparent } no vtp mode

no - このコマンドはVTPモードをデフォルト値にリセットします。

初期設定

Server

コマンド・モード

グローバル・コンフィグ

9.4.5.8 vtp password

このコマンドはVTP管理ドメインのパスワードを構成するために使います。

Syntax
vtp password <password> no vtp password

<password> - VTP管理ドメインのパスワードを構成します(最大長 64 バイト)

no - このコメントはVTPドメインパスワードをデフォルト値にリセットします。

初期設定

None

コマンド・モード

グローバル・コンフィグ

9.4.5.9 vtp pruning

このコマンドはプルーニングを許可するために管理ドメインを構成するために使います。

Syntax
vtp pruning no vtp pruning

no - このコマンドはプルーニングモードをデフォルト値にリセットします。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

9.4.5.10 vtp version

このコマンドはvtpバージョンを構成するために使います。

Syntax
vtp version <1-2> no vtp version

<1-2> - バージョン 1 または 2

no - このコマンドはvtpのバージョンをデフォルト値にリセットします。

初期設定

デフォルトバージョンは 1 です。

コマンド・モード

グローバル・コンフィグ

9.4.5.11 **vtp trunkport**

このコマンドはインターフェイスのすべてのための管理ドメイントランクポートを構成するために使います。

Syntax
vtp trunkport all no vtp trunkport all

no - このコマンドは管理ドメインのトランクポートをデフォルト値へリセットします。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

このコマンドは特定のインターフェイスの管理ドメイントランクポートを構成するために使います。

Syntax
vtp trunkport no vtp trunkport

no - このコマンドは管理ドメインのトランクポートをデフォルト値へリセットします。

初期設定

Disabled

コマンド・モード

インターフェイス・コンフィグ

9.4.6 IGMP Snooping (IGMP スヌーピング)

9.4.6.1 コマンドを表示

9.4.6.1.1 show ip igmp snooping

このコマンドはIGMPスヌーピング情報を表示します。構成された情報はIGMPスヌーピングが有効化されているかとは関係なく表示されます。ステータス情報はIGMPスヌーピングが有効の際のみ表示されます。

Syntax
show ip igmp snooping

初期設定

なし

コマンド･モード

特権EXEC

表示メッセージ

Admin Mode: これはIGMPスヌーピングがスイッチ上でアクティブかどうかを表示します。

Multicast Control Frame Count: CPUによるマルチキャスト制御フレーム数を表示ます

Interfaces Enabled for IGMP Snooping: これはIGMPスヌーピングが有効化されたインターフェイスのリストです。

Vlan Enabled for IGMP Snooping: これはIGMPスヌーピングが有効化されたインターフェイスのリストです。

9.4.6.1.2 show ip igmp snooping mrouter

このコマンドは静的に構成されたか動的に習得されたマルチキャストルータポートまたはマルチキャスト･ルータの構成についての情報を表示します。

Syntax
show ip igmp snooping mrouter [{ vlan <vlanid> | interface [slot/port] }]

<vlanid> - VLAN ID (範囲 1～4094)

slot/port - インターフェイス番号

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

VLAN ID: This displays VLAN ID value.

Slot/port: The インターフェイス番号

Multicast Router Attached: これはインターフェイスがマルチキャストルータポートとして有効化されているかを表示します。

9.4.6.1.3 show ip igmp snooping

このコマンドはIGMPスヌーピング情報を表示します。 構成された情報はIGMPスヌーピングが有効化されているかとは関係なく表示されます。

Syntax
show ip igmp snooping <1-4094>

<1-4094> - VLAN ID(範囲は 1 から 4094)

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

VLAN ID: これはIGMPスヌーピングが有効なVLANのリストです。

IGMP Snooping Admin Mode: これはIGMPスヌーピングがVLANでアクティブかどうかを表示します。

Fast Leave Mode: これはVLANでIGMPスヌーピングFast-Leaveがアクティブかどうかを表示します 。

Group Membership Interval Time: グループメンバー資格の間隔時間とはVLANに参加している特定のインターフェイス上の特定グループからの通知を、エントリからそのインターフェイスを削除するまでスイッチが待つ秒数です。この値は構成できます。

Max Response Time: これはVLANに参加しているインターフェイスでクエリーを送ってからそのインターフェイスの特定グループへの通知を受信しなかった場合に待機する時間を表示しています 。

Multicast Router Expiration Time: VLANに参加しているインターフェイスでクエリーを受信できなければ、そのインターフェイスはマルチキャストルータが付いたインターフェイスのリストから削除されます。

9.4.6.1.4 show ip igmp snooping static

ユーザーは特権モードでIGMPスヌーピング静的情報を表示することができる、すなわちip igmpの 静的スヌーピング特権コマンドを使います。

Syntax
show ip igmp snooping static

初期設定

None

コマンド・モード

特権EXEC, ユーザ EXEC

表示メッセージ

VLAN: L2Mcastグループとして求めるパケットを完全に識別するためにMACアドレスとともに使われるVLAN ID

Mac Address: L2McastグループのMACアドレスが 01:00:5E:xx:xx:xx の形式です。

Port: L2Mcastグループに含めるポートをリストします。

State/ステータス: アクティブなインターフェイス番号がマルチキャストグループに属しています。

9.4.6.2 構成コマンド

9.4.6.2.1 ip igmp snooping

このコマンドはシステムのIGMPスヌーピングを有効化します。デフォルト値は無効です。

Syntax
ip igmp snooping no igmp snooping

no - このコマンドはシステムのIGMPスヌーピングを無効化します。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

9.4.6.2.2 ip igmp snooping groupmembershipinterval

このコマンドはシステムのIGMPグループメンバー資格の時間間隔を設定します。グループメンバー資格時間とは特定インターフェイスの特定グループからの通知を、インターフェイスをエントリから削除するまでスイッチが待つ秒数です。この値はIGMPの最大応答時間値より大きくなければなりません。範囲は 2～3600 秒です。

Syntax
ip igmp snooping groupmembershipinterval <2-3600> no ip igmp snooping groupmembershipinterval

<2-3600> -間隔時間 (範囲 2～3600 秒)

no - このコマンドはシステムのIGMPグループメンバー資格間隔時間を 260 秒に設定します。

初期設定

2260 秒

コマンド・モード

グローバル・コンフィグ, インターフェイス・コンフィグ

9.4.6.2.3 ip igmp snooping interfacemode

このコマンドは選択したインターフェイスのIGMPスヌーピングを有効化します。有効なIGMPスヌーピングのあるインターフェイスがルーティングを有効化した場合やポートチャンネル(LAG)のメンバーに記載されていると、IGMPスヌーピングの機能はインターフェイスで無効化されます。IGMPスヌーピング機能はその後に、ルーティングが無効化された場合やポートチャンネル(LAG)のメンバー資格が有効なIGMPスヌーピングを持つインターフェイスから削除されると、再度有効化されます。

Syntax
ip igmp snooping interfacemode no ip igmp snooping interfacemode

no - このコマンドは選択したインターフェイスのIGMPスヌーピングを無効化します。

初期設定

Disabled

コマンド・モード

インターフェイス・コンフィグ

このコマンドはすべてのインターフェイスのIGMPスヌーピングを有効化します。有効なIGMPスヌーピングのあるインターフェイスがルーティングを有効化した場合やポートチャンネル(LAG)のメンバーに記載されていると、IGMPスヌーピング

の機能性はインターフェイスで無効化されます。IGMPのスヌーピング機能はその後に、ルーティングが無効化された場合やポートチャンネル(LAG)のメンバー資格が有効なIGMPスヌーピングを持つインターフェイスから削除された場合、再度有効化されます。

Syntax
ip igmp snooping interfacemode all

all – すべてのインターフェイス

no - このコマンドはすべてのインターフェイスのIGMPスヌーピングを無効化します。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

9.4.6.2.4 ip igmp snooping mcrtrexpiretime

このコマンドはシステムのマルチキャスト・ルータの有効期限切れ時間を設定します。これはインターフェイスがマルチキャストルータの付いたインターフェイスのリストから削除されるまでにインターフェイスで受信されたクエリーをスイッチが待つ秒数です。範囲は 0～3600 秒です。0 の値は無限の期限切れすなわち期限切れがないことを表します 。

Syntax
ip igmp snooping mcrtrexpiretime <0-3600> no ip igmp snooping mcrtrexpiretime

<0-3600> -期限切れ時間(範囲 0~3600)

no - このコマンドはシステムのマルチキャストルータの現在の期限切れ時間を 0 に設定します。0 の値は無限の期限切れすなわち無期限を示します。

初期設定

0

コマンド・モード

グローバル・コンフィグ, インターフェイス・コンフィグ

9.4.6.2.5 ip igmp snooping max-response-time

このコマンドはシステムのIGMPの最大応答時間を設定します。最大応答時間とはインターフェイスの特定のグループへの通知を受信できなかったからインターフェイスでクエリーを送った後にスイッチが待つ秒数です。この値はIGMPクエリー間隔時間の値より小さくなければなりません。範囲は 1～3599 秒です。

Syntax

```
ip igmp snooping max-response-time <sec>
no ip igmp snooping max-response-time
```

<sec> -最大時間 (範囲 1～3599)

no - このコマンドはシステムのIGMP最大応答時間を 10 秒に設定します。

初期設定

10 秒 コマンド･モード

グローバル･コンフィグ, インターフェイス･コンフィグ.

9.4.6.2.6 ip igmp snooping fast-leave

このコマンドはすべての選択されたインターフェイスかすべてのインターフェイスでのIGMPスヌーピングFast-Leave管理モードを有効化または無効化します。Fast-Leaveを有効化することで、最初にMACベースの一般的なクエリーをインターフェイスへ送り出さずに、マルチキャストグループへのIGMP leaveのメッセージを受信と同時に、転送テーブル･エントリからレイヤー2 のLANインターフェイスをスイッチは削除します 。

Fast-Leave管理モードは、同じレイヤー2 ポートへ接続されていながらそのグループへ向けられたマルチキャストのトラフィック受信に関わる他のホストを防止します。ホストが各レイヤー2LANポートへ接続されているVLAN上でのみ有効化してください。また、Fast-Leave処理はIGMPバージョン 2 のホストのみサポートされています 。

Syntax

```
ip igmp snooping fast-leave
no ip igmp snooping fast-leave
```

no - このコマンドはIGMPスヌーピング高速Leave管理モードを無効化します。

初期設定

Disabled

コマンド･モード

グローバル･コンフィグ, インターフェイス･コンフィグ.

9.4.6.2.7 ip igmp snooping mrouter

このコマンドは選択したインターフェイスをマルチキャストルータインターフェイスとして構成します。マルチキャストルータインターフェイスとして構成された後では、そのインターフェイスはすべてのVLANでマルチキャストルータ･インターフェイスとして扱われます。

Syntax
ip igmp snooping mrouter interface no ip igmp snooping mrouter interface

no - このコマンドは静的構成マルチキャストルータのインターフェイスとしてのステータスを無効化します。

初期設定

Disabled

コマンド･モード

インターフェイス･コンフィグ.

このコマンドはマルチキャストルータモードが有効化されたVLAN ID (<vlanId>) を構成します。

Syntax
ip igmp snooping mrouter <vlanId> no set igmp snooping mrouter <vlanId>

<vlanId> - VLAN ID.

no - このコマンドは静的構成マルチキャストルータのインターフェイスとしてのステータスを無効化します 。

初期設定

Disabled

コマンド･モード

インターフェイス･コンフィグ.

9.4.6.2.8 set igmp

このコマンドは特定のVLANのIGMPスヌーピングを有効化し、それと引き替えにこのVLANに参加しているインターフェイスでのIGMPのスヌーピングを有効化します。

Syntax

```
set igmp <1-4094>
no set igmp <1-4094>
```

<1-4094> - VLAN ID(範囲は 1 から 4094)

no - このコマンドは特定のVLANのIGMPスヌーピングを無効にし、それと引き替えにこのVLANに参加しているインターフェイスでのIGMPのスヌーピングを無効化します。

初期設定

None

コマンド・モード

VLAN データベース

9.4.6.2.9 set igmp groupmembership-interval

このコマンドは特定のVLANのIGMPグループメンバー資格の間隔を設定します。グループのメンバー資格の間隔時間とはVLANに参加している特定のインターフェイスの特定のグループからの通知を、エントリからインターフェイスを削除するまで、スイッチが待つ秒数です。値はIGMP最大応答時間の値より大きくなければなりません。範囲は 2～3600 秒です。

Syntax

```
set igmp groupmembership-interval <1-4094> <2-3600>
no set igmp groupmembershipinterval <1-4094>
```

<1-4094> - VLAN ID(範囲は 1 から 4094)

<2-3600> - グループメンバー資格の間隔時間の範囲は 2～3600 秒です。

no - このコマンドは特定のVLANのIGMPグループメンバー資格の間隔時間をデフォルト値に設定します。

初期設定

260

コマンド・モード

VLAN データベース

9.4.6.2.10 set igmp maxresponse

このコマンドは特定のVLANのIGMP最大応答時間を設定します。最大応答時間とはVLANに参加しているインターフェイスでクエリーを送った後、そのインターフェイスの特定のグループへの通知を受信できなかった場合、スイッチが待つ秒数です。この値はIGMPクエリー間隔時間の値よりも小さくなければなりません 。

Syntax
set igmp maxresponse <1-4094> <1-3599> no set igmp maxresponse <1-4094>

<1-4094> - VLAN ID(範囲は 1 から 4094)

no – このコマンドは特定のVLANのIGMP最大応答時間をデフォルト値に設定します。

初期設定

10

コマンド・モード

VLAN データベース

9.4.6.2.11 . set igmp mcrtexpiretime

このコマンドはマルチキャスト・ルータの有効期限切れ時間を設定します。これはインターフェイスがマルチキャストルータの付いたインターフェイスのリストから削除されるまでにインターフェイスで受信されたクエリーをスイッチが待つ秒数です。範囲は 0～3600 秒です。0 の値は無限の期限切れすなわち無期限を表します 。

Syntax
set igmp mcrtexpiretime <1-4094> <0-3600> no set igmp mcrtexpiretime <1-4094>

<1-4094> - VLAN ID(範囲は 1 から 4094)

<0-3600> - マルチキャストルータの現在の期限切れ時間の範囲は 0～3600 秒です。

no - このコマンドは特定のVLANのIGMPマルチキャストルータの現在の期限切れ時間をデフォルト値へ設定します。

初期設定

10

コマンド・モード

VLAN データベース

9.4.6.2.12 set igmp fast-leave

このコマンドはすべての選択されたインターフェイスか選択されたVLANでのIGMPスヌーピングFast-Leave管理モードを有効化または無効化します。Fast-Leaveを有効化することでVLANに参加しているレイヤー2LANインターフェイスをインターフェイスへMACベースの一般的なクエリーをまず送信することなしにマルチキャストグループへのIGMP leaveのメッセージを受信するとすぐに転送テーブル･エントリからレイヤー2LANのインターフェイスを即時に削除することを可能にします。Fast-Leave管理モードは、同じレイヤー2 ポートへ接続されていながらそのグループへ向けられたマルチキャストのトラフィックの受信に関わる他のホストを防ぐ。ホストが各レイヤー2LANポートへ接続されているVLAN上でだけ有効化する。また、Fast-Leave処理はIGMPバージョン 2 のホストのみサポートされています 。

Syntax
set igmp fast-leave <1-4094> no set igmp fast-leave <1-4094>

<1-4094> - VLAN ID(範囲は 1 から 4094)

no - このコマンドは選択されたVLANのIGMPスヌーピング高速Leaveモードを無効化する。

初期設定

None

コマンド･モード

VLAN データベース

9.4.6.2.13 ip igmp snooping static

ユーザーはグローバルモードに入りインターフェイスを静的なマルチキャストグループに追加できます､ip igmp静的スヌーピングのグローバルモードを使います。

Syntax
ip igmp snooping static <macaddr> vlan <1-4094> interface <slot/port> no ip igmp snooping static <macaddr> vlan <1-4094> interface <slot/port>

<macaddr> - MACアドレス

<1-4094> - VLAN ID(範囲は 1 から 4094)

<slot/port> - インターフェイス番号

no - このコマンドは静的マルチキャストグループからインターフェイスを削除します。

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.4.7 IGMP Snooping Querier (IGMP スヌーピング·クエリア)

9.4.7.1 コマンドを表示

9.4.7.1.1 IGMP snooping querier global info

このコマンドはシステムのIGMPスヌーピング·クエリア·グローバル情報を表示します。

Syntax
show ip igmp snooping querier

初期設定

None

コマンド·モード

特権EXEC、ユーザ EXEC

表示メッセージ

IGMP Snooping Querier Mode: IGMPスヌーピングの管理モード。 デフォルトは無効化です。

Querier Address: 定期的なIGMPクエリーのソースアドレスとして使うためスヌーピング·クエリア·アドレスを指定します。

IGMP Version - 定期的なIGMPクエリーに使われるIGMPプロトコルのバージョンを指定します。

Querier Interval - スヌーピング·クエリアによって送られる定期的なクエリーの間隔を秒数で指定します。クエリー間隔は 1 から 1800 の範囲の値でなければなりません。デフォルトは 60 です 。

Querier Expiry Interval - 最後のクエリア情報が削除された以降の間隔を秒数で指定します。クエリア終了間隔は 60 から 300 の範囲の値でなければなりません。デフォルトは 60 です。

9.4.7.1.2 Display IGMP snooping querier vlan info

このコマンドはシステムのIGMPスヌーピング･クエリア･グローバル情報を表示します。

Syntax
show ip igmp snooping querier vlan <1-4094>

初期設定

なし

コマンド･モード

特権EXEC、ユーザ EXEC

表示メッセージ

IGMP Snooping Vlan Mode: スイッチのためのIGMPスヌーピングの管理モードを表示します。

Querier Election Participation Mode -VLANのクエリア選択参加モードを表示します。このモードを無効化すると、VLANの同じバージョンの別のクエリアを見たときにスヌーピングクエリアは非クエリア状態に移ってしまいます。このモードが有効化されている場合のみ、スヌーピング･クエリアは、IPアドレスがクエリアとして選択され、そのVLANでのクエリアとして稼働しているようなクエリア選択に参加できます。他方のクエリアは非クエリア状態へ移行します。

Querier Vlan Address: 特定のVLAN上で送られる定期的なIGMPクエリーのソースアドレスとして使われるスヌーピング･クエリア･アドレスを表示します。.

Operational State: VLANでのMLDスヌーピングクエリアの稼働ステータスを指定します。

Operational Version: クエリアの稼働MLDプロトコルのバージョンを表示します。

9.4.7.1.3 IGMP snooping querier detail information

このコマンドはシステムのMLDスヌーピングクエリア情報のすべてを表示します。

Syntax
show ip igmp snooping querier detail

初期設定

なし

コマンド・モード

特権EXEC、ユーザ EXEC

表示メッセージ

IGMP Snooping Querier Mode: IGMPスヌーピングの管理モード。 デフォルトは無効化です。

Querier Address - 定期的なIGMPクエリーのソースアドレスとして使うためスヌーピング・クエリア・アドレスを指定します。

IGMP Version– 定期的なIGMPクエリーに使われるIGMPプロトコルのバージョンを指定します。

Querier Interval - スヌーピング・クエリアによって送られる定期的なクエリーの間の間隔を秒数で指定します。クエリー間隔は 1 から 1800 の範囲の値でなければなりません。デフォルトは 60 です。

Querier Expiry Interval - 最後のクエリア情報が削除された以降の間隔を秒数で指定します。クエリア終了間隔は 60 から 300 の範囲の値でなければなりません。デフォルトは 60 です。

Last Querier Address - クエリーがVLANでスヌープされた最後のクエリアのIPアドレスを表示します。

9.4.7.2 構成コマンド

9.4.7.2.1 IGMP snooping querier admin mode

ユーザーはCLIグローバル・コンフィグモードに入り、IGMPスヌーピングクエリア管理モードをセットできます、ip igmpスヌーピングクエリアグローバル・コンフィグコマンドを使います。no ip igmp snooping querierにより無効化します。

Syntax
ip igmp snooping querier no ip igmp snooping querier

初期設定

無効

コマンド・モード

グローバル・コンフィグ

9.4.7.2.2 IGMP snooping querier address

ユーザーはCLIグローバル・コンフィグモードに入りIGMPスヌーピングクエリアアドレスをセットできます、ip igmp snooping querier address <ip-address>グローバル・コンフィグコマンドを使います。デフォルト値のゼロへ戻すにはno ip igmp snooping querier addressを使います。

Syntax
ip igmp snooping querier address <ip-address> no ip igmp snooping querier address

初期設定

0

コマンド・モード

グローバル・コンフィグ

9.4.7.2.3 IGMP snooping querier query-interval

ユーザーはCLIグローバル･コンフィグモードに入り、IGMPスヌーピングクエリアのクエリー間隔を設定します、ip igmp snooping querier query-interval <1-1800>グローバル･コンフィグコマンドを使います。 デフォルトのゼロへ戻すにはno ip igmp snooping querier query-intervalを使います。

Syntax
ip igmp snooping querier query-interval <1-1800> no ip igmp snooping querier query-interval

初期設定

0

コマンド･モード

グローバル･コンフィグ

9.4.7.2.4 IGMP snooping querier querier-expiry-interval

ユーザーはCLIグローバル･コンフィグモードに入り、IGMPスヌーピングクエリア･クエリア期限切れ間隔をセットできます、ip igmp snooping querier querier-expiry-interval <60-300>グローバル･コンフィグコマンドを使います。デフォルトのゼロに戻すにはno ip igmp snooping querier query-intervalを使います。

Syntax
ip igmp snooping querier querier-expiry-interval <60-300> no ip igmp snooping querier querier-expiry-interval

初期設定

0

コマンド･モード

グローバル･コンフィグ

9.4.7.2.5 IGMP snooping query verion

ユーザーはCLIグローバル･コンフィグモードに入りIGMPスヌーピングクエリアのバージョンをセットできます。ip igmp snooping querier version <1-2>グローバル･コンフィグコマンドを使います。デフォルトのゼロに戻すにはno ip igmp snooping querier versionを使います。

Syntax
ip igmp snooping querier version <1-2> no ip igmp snooping querier version

初期設定

0

コマンド･モード

グローバル･コンフィグ

9.4.7.2.6 IGMP snooping querier vlan admin mode

ユーザーはCLIグローバル･コンフィグモードに入りIGMPスヌーピングクエリアVLAN管理モードをセットできます､ip igmp snooping querier vlan <1-4094>グローバル･コンフィグコマンドを使います。デフォルトのゼロに戻すにはno ip igmp snooping querier vlan <1-4094>を使います。」

Syntax
ip igmp snooping querier vlan <1-4094> no ip igmp snooping querier vlan <1-4094>

初期設定

0

コマンド･モード

グローバル･コンフィグ

9.4.7.2.7 IGMP snooping querier vlan address

ユーザーはCLIグローバル･コンフィグモードに入り、IGMPスヌーピングクエリアVLAN選択参加モードをセットできます、ip igmp snooping querier vlan <1-4094> election-participateグローバル･コンフィグコマンドを使います。無効に戻すにはno ip igmp snooping querier vlan <1-4094> election-participateを使います。

Syntax
ip igmp snooping querier vlan <1-4094> address <ip-address> no ip igmp snooping querier vlan <1-4094> address

初期設定

0

コマンド･モード

グローバル･コンフィグ

9.4.7.2.8 IGMP snooping querier vlan election mode

ユーザーはCLIグローバル･コンフィグモードに入りIGMPスヌーピングクエリアVLAN選択参加モードをセットできます､ip igmp snooping querier vlan <1-4094> election-participateグローバル･コンフィグコマンドを使います｡無効へ戻すにはno ip igmp snooping querier vlan <1-4094> election-participateを使います｡

Syntax
ip igmp snooping querier vlan <1-4094> election-participate no ip igmp snooping querier vlan <1-4094> election-participate

初期設定

0

コマンド･モード

グローバル･コンフィグ

9.4.8 MLD スヌーピング

9.4.8.1 コマンドを表示

9.4.8.1.1 show ipv6 mld snooping

ユーザーはCLI特権モードに入りすべてのmld スヌーピング情報を入手できます、show ip mld snooping特権コマンドを使います。

Syntax
show ipv6 mld snooping [<slot/port>|<vlan-id>]

初期設定

なし

コマンド・モード

特権EXEC、ユーザ EXEC

表示メッセージ

オプションの引数<slot/port> または <vlanid> が使われていなければ、コマンドは次の情報を表示します。

Admin Mode: MLDスヌーピングがスイッチ上でアクティブかどうかを示します。

Interfaces Enabled for MLD Snooping: MLDスヌーピングが有効化されたインターフェイス

MLD Control Frame Count: CPUに処理されるMLD制御フレームの数を表示します。

VLANs Enabled for MLD Snooping: MLDスヌーピングが有効なVLAN

<slot/port>の値を特定するときは、次の情報が表示されます:

MLD Snooping Admin Mode: MLDスヌーピングがインターフェイス上でアクティブか否かを示します。

Fast Leave Mode: MLDスヌーピングFast-Leaveがインターフェイスでアクティブか否かを示します 。

Group Membership Interval: インターフェイスへ参加している特定のインターフェイスの上の特定のグループからの通知を、エントリからインターフェイスを削除するまで、スイッチが待つ秒数。この値が構成できます。

Max Response Time: MLDスヌーピングが有効になるインターフェイス。

Multicast Router Present Expiration Time: インターフェイス上で参加しているインターフェイスをマルチキャストルータが付いたインターフェイスのリストから削除する前まで待つ時間です。クエリーが受信されたらインターフェイスは削除されます。この値は構成できます。

<vlanid>の値を指定すると、次の情報が現れます;

VLAN ID: VLAN ID

MLD Snooping Admin Mode: MLDスヌーピングがVLANでアクティブかどうかを示します。

Fast Leave Mode: MLDスヌーピング高速LeaveがVLANでアクティブかどうかを示します 。

Group Membership Interval: VLANに参加している特定のインターフェイスの特定のグループからの通知を、エントリからインターフェイスを削除するまでスイッチが待つ秒数。この値は構成できます。

Max Response Time: MLDスヌーピングが有効なVLAN

Multicast Router Present Expiration Time: VLANに参加しているインターフェイスをマルチキャストルータが付いたインターフェイスのリストから削除するまで待つ時間。インターフェイスはクエリーが受信されなければ削除されます。この値は構成できます。

9.4.8.1.2 show ipv6 mld snooping mroute

ユーザーはCLI特権モードに入り静的に構成されたルータが付くマルチキャストについての情報を表示できます、show ipv6 mld snooping mrouter特権コマンドを使います。

Syntax
show ipv6 mld snooping mrouter

初期設定

なし

コマンド・モード

特権EXEC、ユーザ EXEC

表示メッセージ

Interface: マルチキャストルータの情報が表示されるインターフェイスを表示する。

Multicast Router Attached: マルチキャストルータがインターフェイス上で静的に有効になるかどうかを示す。

VLAN ID: インターフェイスがメンバーのVLANのリストを表示。

9.4.8.1.3 show ipv6 mld snooping mrouter interface

有効ユーザーはCLI特権モードに入り、静的構成マルチキャストのルータ付きインターフェイスについての情報を表示する。

Syntax
show ipv6 mld snooping mrouter interface <slot/port>

初期設定

なし

コマンド・モード

特権EXEC、ユーザ EXEC

表示メッセージ

Interface : マルチキャストルータの情報が表示されるインターフェイスを表示する

Multicast Router Attached: マルチキャストルータがインターフェイス上で静的に有効になるかどうかを示す。

VLAN ID: インターフェイスがメンバーのVLANのリストを表示

9.4.8.1.4 show ipv6 mld snooping mrouter vlan

ユーザーはCLI特権モードへ進み、静的構成マルチキャスト・ルーターに接続されたインターフェイスの情報を表示できます。 show ipv6 mld snooping mrouter vlan特権コマンドを使用します。

Syntax
show ipv6 mld snooping mrouter vlan <slot/port>

初期設定

なし

コマンド・モード

特権EXEC、ユーザ EXEC

表示メッセージ

VLAN ID: インターフェイスがメンバーのVLANのリストを表示します。

Interface: マルチキャストルータの情報が表示されるインターフェイスを表示する

9.4.8.1.5 show ipv6 mld snooping static 。

ユーザーは特権モードに入り、MLD静的スヌーピング情報を表示します、show ipv6 mld snooping static特権コマンドを使います。.

Syntax
show ipv6 mld snooping static

初期設定

なし

コマンド・モード

特権EXEC, ユーザ EXEC

表示メッセージ

VLAN: L2Mcastグループにパケットを完全に識別するためのMACアドレスとともに使うVLAN ID.

MAC Address: 33:33:xx:xx:xx:xxの形式のL2McastグループのMACアドレス

Port: L2Mcastグループへ含めるポートのリスト

State: アクティブインターフェイス番号はマルチキャストグループに属します。

9.4.8.1.6 show mac-address-table mldsnooping

ユーザーはCLI特権モードに入り、マルチキャスト転送データベース(MFDB)のMLDスヌーピングエントリを表示します、show mac-address-table mldsnooping特権コマンドを使います。

Syntax
show mac-address-table mldsnooping

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

MAC Address: スイッチが転送かフィルタリング情報を持つマルチキャストのMACアドレス。フォーマットは 2 桁の 16 進法の数字がコロンで区切られています、たとえば 33:33:45:67:89:AB です。.

Type: エントリのタイプ、これは静的(ユーザーにより追加)または動的(習得プロセスかプロトコルの結果としてテーブルに追加された)です。

Description: マルチキャストテーブルエントリのテキスト記述

Interfaces: 転送(Fwd:)とフィルタリング(Flt:)に指定されるインターフェイスのリスト。

9.4.8.2 **構成コマンド**

9.4.8.2.1 ip mld snooping

ユーザーはCLIグローバル/インターフェイス・コンフィグモードに入り、システム上かインターフェイスのMLDスヌーピングをセットできます、ipv6 mld snoopingグローバル/インターフェイス・コンフィグコマンドを使います。 システムまたはインターフェイスのMLDスヌーピングを無効につするにはno ipv6 mld snoopingを使います。

Syntax
ip mld snooping no ip mld snooping

初期設定

無効

コマンド・モード

グローバル・コンフィグ、インターフェイス・コンフィグ

9.4.8.2.2 ipv6 mld snooping interfacemode

ユーザーはCLIグローバル/インターフェイス・コンフィグモードに入り、ひとつまたはすべてのインターフェイスのMLDスヌーピングを設定します。ipv6 mld snooping interfacemodeグローバル/インターフェイス・コンフィグコマンドを使います。すべてのインターフェs.

Syntax
ipv6 mld snooping interfacemode <all> no ipv6 mld snooping interfacemode <all>

初期設定

無効

コマンド・モード

グローバル・コンフィグ、インターフェイス・コンフィグ

9.4.8.2.3 ipv6 mld snooping fast-leave

ユーザーはCLIグローバル/インターフェイス･コンフィグモードに入り､選択したインターフェイスかすべてのインターフェイスのMLDスヌーピングFast-leave管理モードをセットできます､

ipv6 mld snooping fast-leaveグローバル/インターフェイス･コンフィグコマンドを使います。MLDスヌーピングFast-Leave管理モードを無効化するにはno ipv6 mld snooping fast-leaveを使います｡.

Syntax
ipv6 mld snooping fast-leave no ipv6 mld snooping fast-leave

初期設定

無効

コマンド･モード

グローバル･コンフィグ、インターフェイス･コンフィグ

9.4.8.2.4 ipv6 mld snooping groupmembershipinterval

ユーザーはCLIグローバル/インターフェイス･コンフィグモードに入り､ひとつまたはすべてのインターフェイスのMLD得ループメンバー資格間隔時間をセットできます､ipv6 mld snooping groupmembershipinterval <2-3600>を使います｡デフォルト値の 260 に戻すにはno ipv6 mld snooping groupmembershipintervalを使います。

Syntax
ipv6 mld snooping groupmembershipinterval <2-3600> no ipv6 mld snooping groupmembershipinterval

初期設定

260

コマンド･モード

グローバル･コンフィグ、インターフェイス･コンフィグ

9.4.8.2.5 ipv6 mld snooping max-response-time

1 ユーザーはCLIインターフェイスグローバル/インターフェイス･コンフィグモードに入り､特定のインターフェイス上のシステムへのMLD最大応答時間をセットできます｡ipv6 mld snooping max-response-time <1-3599>を使います｡デフォルトの 10 に戻すにはno ipv6 mld snooping max-response-timeを使います ｡

Syntax
ipv6 mld snooping max-response-time <1-3599> no ipv6 mld snooping max-response-time

初期設定

10

コマンド･モード

グローバル･コンフィグ､ インターフェイス･コンフィグ

9.4.8.2.6 ipv6 mld snooping mcrtrexpiretime

ユーザーはCLIインターフェイス グローバル/インターフェイス･コンフィグモードに入り､特定のインターフェイスのシステムのためのマルチキャストルータの有効期限切れ時間をセットできます｡ipv6 mld snooping mcrtrexpiretime <0-3600>グローバル/インターフェイス･コンフィグコマンドを使います｡デフォルトの 0 に戻すにはno ipv6 mld snooping mcrtrexpiretimeを使います ｡.

Syntax
ipv6 mld snooping mcrtrexpiretime <0-3600> no ipv6 mld snooping mcrtrexpiretime

初期設定

0

コマンド･モード

グローバル･コンフィグ､ インターフェイス･コンフィグ

9.4.8.2.7 ipv6 mldスヌーピングmrouterインターフェイス

ユーザーはCLIインターフェイス･コンフィグモードに入り､ルータ付きのマルチキャストインターフェイスとしてインターフェイスを構成することも､マルチキャストルータ付きのモードが有効なVLANのためのVLAN IDを構成することもできます､ipv6 mld snooping mrouter interface interface|<vlanid>インターフェイス･コンフィグコマンドを使います。インターフェイスまたはVLANのためのマルチキャスト付きモードを無効化するにはno ipv6 mld snooping mrouter interface|<vlanid>を使います。

Syntax
ipv6 mld snooping mrouter interface interface|<vlanId> no ipv6 mld snooping mrouter interface|<vlanId>

初期設定

なし

コマンド･モード

インターフェイスの構成

9.4.8.2.8 ipv6 mld静的スヌーピング

ユーザーはグローバルモードに入りipv6 マルチキャストグループにポートを追加できます､ipv6 mld snooping staticグローバルコマンドを使います。

Syntax
ipv6 mld snooping static <macaddr> vlan <vlan-id> interface <slot/port> no ipv6 mld snooping static <macaddr> vlan <vlan-id> interface <slot/port>

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.4.8.2.9 set mld

2　　ユーザーはCLI VLANモードに入り､特定のVLANのMLDスヌーピングをセットできます｡set mld <vlanid>VLAN構成コマンドを使います｡特定のVLANのMLDスヌーピングを無効化するにはno set mld <vlanid>wp を使います 。

Syntax
set mld <vlanid> no set mld <vlanid>

初期設定

無効化する

コマンド･モード

VLANデータベース

9.4.8.2.10 set mld fast-leave

3　　ユーザーはCLI VLAN構成モードに入り､特定のVLANのMLDスヌーピング高速leave管理モードをセットできます｡set mld fast-leave <vlanid> VLAN構成コマンドをつかいます｡MLDスヌーピング高速leave管理モードを無効化するにはno set mld fast-leave <vlanid>を使います 。

Syntax
set mld fast-leave <vlanid> no set mld fast-leave <vlanid>

初期設定

無効化する

コマンド･モード

VLANデータベース

9.4.8.2.11 set mld groupmembership-interval

ユーザーはCLI VLAN構成モードに入り特定のVLANのMLDグループメンバー資格の間隔時間をセットできます。set mld groupmembership-interval <vlanid> <2-3600> VLAN構成コマンドを使います。デフォルトの 260 に戻すにはno set mld groupmembership-interval <vlanid>を使います。

Syntax
set mld groupmembership-interval <vlanid> <2-3600> no set mld groupmembership-interval <vlanid>

初期設定

260

コマンド・モード

VLANデータベース

9.4.8.2.12 set mld maxresponseコマンド

ユーザーはCLI VLAN構成モードに入り特定のVLANのMLDグループメンバー資格の間隔時間をセットできます。set mld max-response-time <vlanid> <2-3599> **VLAN構成コマンドを使います。デフォルトの 260 に戻すにはno set mld** max-response-time <vlanid>**を使います**

Syntax
set mld max-response-time <vlanid> <1-3599> no set mld max-response-time <vlanid>

初期設定

10

コマンド・モード

VLANデータベース

9.4.8.2.13 set mld mcrtrexpiretime

ユーザーはCLIインターフェイスVLAN構成モードに入り、特定のVLANのマルチキャスト･ルータの現在の期限切れ時間をセットできます。set mld mcrtrexpiretime <vlanid> <0-3600>VLAN構成コマンドを使います。デフォルトのゼロに戻すにはno set mld mcrtrexpiretime <vlanid>を使います。

Syntax
set mld mcrtrexpiretime <vlanid> <0-3600> no set mld mcrtrexpiretime <vlanid>

初期設定

0

コマンド･モード

VLANデータベース

9.4.9 MLD スヌーピングクエリア

9.4.9.1 コマンドを表示

9.4.9.1.1 show ipv6 mld snooping querier

このコマンドはシステムのMLDスヌーピングクエリアグローバル情報を表示します。

Syntax
show ipv6 mld snooping querier

初期設定

なし

コマンド・モード

特権EXEC、ユーザ EXEC

表示メッセージ

MLD Snooping Querier Mode: スヌーピングクエリアアドレスを定期的なMLDクエリーのソースアドレスとして使われるように指定します。このアドレスはクエリーが送られるVLANにアドレスが構成されていないときに使われます。

Querier Address: 定期的なMLDクエリーのソースアドレスに使われるスヌーピングクエリアアドレスを指定します。このアドレスはクエリーが送られるVLANにアドレスが構成されていないときに使われます。

MLD Version: 定期的なMLDクエリーに使われるMLDプロトコルバージョンを指定します。

Querier Interval - スヌーピング・クエリアによって送られる定期的なクエリーの間の間隔を秒数で指定します。クエリー間隔は 1 から 1800 の範囲の値でなければなりません。デフォルトは 60 です。

Querier Expiry Interval – 最後のクエリア情報が削除された以降の間隔を秒数で指定します。クエリア終了間隔は 60 から 300 の範囲の値でなければなりません。デフォルトは 60 です。

9.4.9.1.2 show ipv6 mld snooping querier vlan

このコマンドはシステムのMLDスヌーピングクエリアVLAN情報を表示します。

Syntax
show ipv6 mld snooping querier vlan <1-4094>

初期設定

なし

コマンド・モード

特権EXEC、ユーザ EXEC

表示メッセージ

MLD Snooping Querier Vlan Mode: VLANのクエリア選択参加モードを表示します。このモードを無効化すると、VLANの同じバージョンの別のクエリアを見たときにスヌーピングクエリアは非クエリア状態に移ります。このモードが有効化されている場合のみ、スヌーピング・クエリアは、IPアドレスがクエリアとして選択され、そのVLANでのクエリアとして稼働しているようなクエリア選択に参加できます。他方のクエリアは非クエリア状態へ移行します 。

Querier Vlan Address: 特定のVLANで送信される定期的なMLDクエリーのソースアドレスに使われるスヌーピングクエリアアドレスを表示します。

Operational State: VLANでのMLDスヌーピングクエリアの稼働ステータスを指定します。

Operational Version: クエリアの稼働MLDプロトコルのバージョンを表示します。

9.4.9.1.3 MLDスヌーピングクエリアの情報のすべてを表示します

このコマンドはシステムのMLDスヌーピングクエリア情報のすべてを表示します。

Syntax
show ipv6 mld snooping querier detail

初期設定

なし

コマンド・モード

特権EXEC、ユーザ EXEC

表示メッセージ

MLD Snooping Querier Mode: MLDスヌーピングの管理モード。デフォルトは無効化です。

Querier Address: 定期的なMLDクエリーのソースアドレスに使われるスヌーピングクエリアアドレスを指定します

このアドレスはクエリーが送られるVLANにアドレスが構成されていないときに使われます。

MLD Version: 定期的なIGMPクエリーに使われるMLDプロトコルバージョンを指定します。

Querier Interval - スヌーピング･クエリアによって送られる定期的なクエリーの間隔を秒数で指定します｡クエリー間隔は 1 から 1800 の範囲の値でなければなりません｡デフォルトは 60 です ｡

Querier Expiry Interval – 最後のクエリア情報が削除された以降の間隔を秒数で指定します｡クエリア終了間隔は 60 から 300 の範囲の値でなければなりません｡デフォルトは 60 です｡

Last Querier Address: クエリーがVLANでスヌープされた最後のクエリアのIPアドレスを表示します｡.

9.4.9.2 構成コマンド

9.4.9.2.1 ipv6 mld snooping querier

ユーザーはCLIグローバル･コンフィグモードに入り､MLDスヌーピングクエリア管理モードをセットできます､ipv6 mld snooping querierグローバル･コンフィグコマンドを使います｡no ipv6 mld snooping querierで無効化します｡

Syntax
ipv6 mld snooping querier no ipv6 mld snooping querier

初期設定

無効化する

コマンド･モード

グローバル･コンフィグ

9.4.9.2.2 ipv6 mld snooping querier address

4 ユーザーはCLIグローバル･コンフィグモードに入り､MLDスヌーピングクエリアアドレスをセットできます､ipv6 mld snooping querier address <ipv6-address>グローバル･コンフィグコマンドを使います｡デフォルトのゼロに戻すにはno ipv6 mld snooping querier address <ipv6-address>を使います｡

Syntax
ipv6 mld snooping querier address <ipv6-address> no ipv6 mld snooping querier address <ipv6-address>

初期設定

0

コマンド･モード

グローバル･コンフィグ

9.4.9.2.3 ipv6 mld snooping querier querier-interval

ユーザーはCLIグローバル･コンフィグモードに入り､MLDスヌーピングクエリア間隔をセットできます｡ipv6 mld snooping querier querier-interval <1-1800>グローバル･コンフィグコマンドを使います｡デフォルトのゼロへ戻すにはno ipv6 mld snooping querier querier-interval <1-1800>を使います ｡

Syntax
ipv6 mld snooping querier querier-interval <1-1800> no ipv6 mld snooping querier querier-interval

初期設定

0

コマンド･モード

グローバル･コンフィグ

9.4.9.2.4 ipv6 mld snooping querier querier-expiry-interval

5 ユーザーはCLIグローバル･コンフィグモードに入りMLDスヌーピングクエリア期限切れ間隔をセットできます､ipv6 mld snooping querier querier-expiry-interval <60-300>グローバル･コンフィグコマンドを使います｡デフォルトのゼロに戻すにはno ipv6 mld snooping querier querier-expiry-interval <60-300>を使います ｡.

Syntax
ipv6 mld snooping querier querier-expiry-interval <60-300> no ipv6 mld snooping querier querier-expiry-interval

初期設定

0

コマンド･モード

グローバル･コンフィグ

9.4.9.2.5 ipv6 mld snooping querier vlan

6　ユーザーはCLIグローバル･コンフィグモードに入り､MLDスヌーピングクエリアVLAN管理モードをセットできます､ipv6 mld snooping querier vlan <1 4094>グローバル･コンフィグコマンドを使います。無効に戻すにはno ipv6 mld snooping querier vlan <1-4094>を使います。

Syntax
ipv6 mld snooping querier vlan <1-4094> no ipv6 mld snooping querier vlan <1-4094>

初期設定

無効化する

コマンド･モード

グローバル･コンフィグ

9.4.9.2.6 ipv6 mld snooping querier vlan

7　ユーザーはCLIグローバル･コンフィグモードに入り､MLDスヌーピングクエリアVLANアドレスを設定します､ipv6 mld snooping querier vlan <1-4094> address <ip-address>グローバル･コンフィグコマンドを使います。デフォルトのゼロに戻すにはno ipv6 mld snooping querier vlan <1-4094> address <ip-address>を使います。

Syntax
ipv6 mld snooping querier vlan <1-4094> address <ip-address> no ipv6 mld snooping querier vlan <1-4094> address <ip-address>

初期設定

無効化する

コマンド･モード

グローバル･コンフィグ

9.4.9.2.7 MLD snooping querier vlan election mode

ユーザーはCLIグローバル・コンフィグモードに入り、MLDスヌーピングクエリアVLAN選択参加モードを設定します、ipv6 mld snooping querier vlan <1-4094> election-participateグローバル・コンフィグコマンドを使います。無効に戻すにはno ipv6 mld snooping querier vlan <1-4094> election-participateを使います。

Syntax
ipv6 mld snooping querier vlan <1-4094> election-participate no ipv6 mld snooping querier vlan <1-4094> election-participate

初期設定

無効化する

コマンド・モード

グローバル・コンフィグ

9.4.10 ポートチャネル

9.4.10.1 show port-channel

このコマンドは個々のポートチャネルのサマリのほかすべてのポートチャネル (LAG) の静的機能を表示します。

Syntax
show port-channel

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Static Capability: デバイスの静的機能が有効であるかを示します。

各ポートチャネルでは、以下の情報が表示されます:

Logical Interface: 論理スロットおよび論理ポートを示します。

Port-Channel Name: ポートチャネル名を示します。

Link State: リンクがアップであるかダウンであるかを示します。

Mbr Ports: ポートチャネルのメンバーであるポートを、スロット／ポートの表記で列記します。

Active Ports: ポートチャネルにアクティブに参加しているポートを列記します。

このコマンドはスイッチ上のすべてのポートチャンネル(LAG)の概要を表示します。

Syntax
show port-channel {<slot/port> | all}

<slot/port> - ポートチャネルのインタフェイス番号

all – すべてのポートチャネルのインタフェイス

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Log. Intf: 論理スロットと論理ポート

Port-Channel Name: ポートチャネル (LAG) 名。最大 15 文字の英数字を入力できます。

Link : リンク･ステータス - リンクがアップかダウンかを示す。

Admin Mode: 有効化または無効化します。 デフォルト設定は有効化されている。

Link Trap Mode: リンクステータスを変更した場合、トラップを送信するかを設定します。 デフォルト設定は有効化されている。

STPモード: ポートまたはポートチャンネル(LAG)に関連付けられたスパニングツリープロトコル管理モード。可能な値は:
Disable:スパニングツリーはポートには無効です 。
Enable: スパニングツリーはこのポートには有効です。(デフォルト値)
Mbr Ports: ポートチャネル (LAG) のメンバーであるポートをスロット／ポートの表記で列記します。指定ポートチャネル (LAG) には最大 8 つのポートを割り当てることができます。

Port Speed: ポートチャネルのポートの速度。

Type: 指定のポートチャネル (LAG) を静的または動的に管理するかを設定するステータスを示します。値は、ポートチャネルを静的に管理する場合はStatic、動的に管理する場合はDynamicとなります。

Port Active: ポートチャネル (LAG) にアクティブに参加するポートを列記します。

9.4.10.2 **show lacp interface**

このコマンドは特定のインターフェイスまたはすべてのインターフェイスのLACP状態の概要を表示します。

Syntax
show lacp interface {<slot/port> | all}

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Intf: インタフェイス番号を示します。

Role: インターフェイスの役割。以下のいずれかとなります。

- **Actor:** LACPネゴシエーションに参加するローカルデバイス
- **Partner:** LACPネゴシエーションに参加するリモートデバイス

Exp: 期限切れの状態。Yesはactorまたはpartnerが期限切れの状態であることを示します。Noはactorまたはpartnerが期限切れの状態ではないことを示します。

Def: デフォルト。Yesはactorの受信マシンがデフォルトの動作partnerの情報を使用しており、partnerについて管理設定していることを示します。Noは使用している動作partnerの情報をLACP PDUで受信していることを示します。

Dist: 送信フレームの提供。Noはリンクへの送信フレーム提供が現在無効であり、有効化できないことを示します。それ以外の場合、値はYesとなります。

Col: 受信フレームの取得。Yesはリンクへの受信フレーム取得が現在有効であり、無効化できないことを示します。それ以外の場合、値はNoとなります。

Syn: 同期。Yesの場合、リンクは「同期中」となります。正しいリンク集約グループへ割り当てられ、該当する集約にグループが関連付けられ、リンク集約グループがシステムIDおよび送信された動作キー情報と照合されます。Noの場合、リンクは現在「非同期」となり、正しい集約でないことを示します。

Aggr: 集約化ポートへの集約が可能である(Yes)か、個別リンクでのみ動作する(No)かを示します。

Timeout: LACPタイムアウト設定。指定されたLACPタイムアウト設定により、低速または高速の送信レートでLACP PDUの定期送信が行われます(Long TimeoutまたはShort Timeout)。

Activity: actorまたはpartnerのポート動作。Passiveはpartnerの制御値がActiveでない場合LAC PDUの送信を行わないことを示します。Activeはpartnerの制御値に関係なくプロトコルに参加することを示します。

9.4.10.3 **port-channel**

このコマンドは新しいポートチャンネル(LAG)を構成しそれに対する論理的なスロットとポート番号を作ります。

注記: ポートチャネルにポートを追加する前に、ポートの物理モードを設定してください。詳細については「**speed-duplex**」コマンドを参照してください。

Syntax
port-channel <name> no port-channel {<slot/port> | all}

<logical slot/port> - ポートチャネルのインタフェイス番号

<name> - ポートチャネル名 (最大 15 文字の英数字)

all - すべてのポートチャネルのインタフェイス

no - ポートチャネルを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

コマンドの使用法

ユーザーが作成できるポートチャネルの最大数は 64、1 ポートチャネルあたりの最大メンバー数は 6 です。

9.4.10.4 **port-channel adminmode all**

このコマンドによりすべての設定ポートチャネルに同じ管理モード設定を適用します。

Syntax
port-channel adminmode all no port-channel adminmode all

no - このコマンドでポートチャネル (LAG) を無効化します。すべての設定ポートチャネルに同じ管理モード設定を適用します。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

9.4.10.5 **port-channel linktrap**

このコマンドによりポートチャネル (LAG) のリンクトラップ通知を有効化します。設定ポートチャネルで、インタフェイスは論理スロットおよび論理ポートとなります。allオプションではすべての設定ポートチャネルに同じ管理モード設定を適用できます。

Syntax
port-channel linktrap {<slot/port> | all} no port-channel linktrap {<slot/port> | all}

<slot/port> - ポートチャネルのインタフェイス番号

all - すべてのポートチャネルのインタフェイス

no - このコマンドによりポートチャネル (LAG) のリンクトラップ通知を無効化します。設定ポートチャネルで、インターフェイスは論理スロットおよび論理ポートとなります。allオプションによりすべての設定ポートチャネルに同じ管理モード設定を適用できます。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

9.4.10.6 **port-channel name**

このコマンドによりポートチャネル (LAG) 名を定義します。設定ポートチャネルで、インターフェイスは論理スロットおよび論理ポートとなり、名前は最大 15 文字の英数字となります。このコマンドによりポートチャネル作成時にそのポートチャネルに関連する名前を修正します。

Syntax
port-channel name {<slot/port> | all} <name>

<slot/port> - ポートチャネルのインタフェイス番号

all - すべてのポートチャネルのインタフェイス

<name> -設定ポートチャネル名 (最大 15 字)

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.4.10.7 port-channel load-balance

このCLIのコマンドで、すべてのポートチャネルの負荷分散モードを設定します。パラメータsrc-mac | dst-mac | dst-src-mac | src-ip | dst-ip| dst-src-ipは、ポートチャネルの負荷分散設定に使用するモードを示します。

Syntax
port-channel load-balance all { src-mac| dst-mac | dst-src-mac | src-ip | dst-ip| dst-src-ip } no port-channel load-balance all

src-mac - 送信元MACアドレスにモードを設定します。

dst-mac - モードを送信先MACアドレスに設定する。

dst-src-mac - モードを送信元と送信先MACアドレスに設定する。

src-ip - モードを送信元IPアドレスに設定する。

dst-ip - モードを送信先IPアドレスに設定する。

dst-src-ip - モードを送信元と送信先IPアドレスに設定する。

no - モードをデフォルト値に戻します 。

初期設定

dst-src-ip

コマンド・モード

グローバル・コンフィグ

9.4.10.8 adminmode

このコマンドによりポートチャネル (LAG) のメンバーを有効化します。設定ポートチャネルで、インターフェイスは論理スロットおよび論理ポートとなります。

Syntax
adminmode no adminmode

no - このコマンドにより設定ポートチャネル (LAG) を無効化します

初期設定

有効

コマンド・モード

インターフェイス・コンフィグ

9.4.10.9 staticcapability

このコマンドにより静的ポートチャネル (静的リンク集約:LAG) のサポートを有効化します。デフォルトではすべてのポートチャネルの静的機能は無効化されています。設定ポートチャネルで、インターフェイスは論理スロットおよび論理ポートとなります。

Syntax
staticcapability no staticcapability

no - このコマンドにより静的ポートチャネルのサポートを無効化します。

初期設定

無効

コマンド・モード

インターフェイス・コンフィグ

9.4.10.10 lacp

このコマンドはポートのリンクアグリゲーション制御プロトコル(LACP)を有効化します。

Syntax
lacp no lacp

no - このコマンドは 1 個のポートにおいてリンクアグリゲーション制御プロトコル (LACP)を無効化します。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

このコマンドはすべてのポートのリンクアグリゲーション制御プロトコル(LACP)を有効化します。.

Syntax
lacp all no lacp all

all -すべてのインターフェイス

no - このコマンドはすべてのポートにおいてリンクアグリゲーション制御プロトコル (LACP)を無効化します。

デフォルト設定

有効化

コマンドモード

グローバル･コンフィグ

9.4.10.11 **channel-group**

このコマンドによりポートチャネル (LAG) にポートを 1 個追加します。最初のインターフェイスは設定ポートチャネルの論理スロット番号および論理ポート番号となります。

注記: ポートチャネルにポートを追加する前に、ポートの物理モードを設定してください。詳細については「speed-duplex」コマンドを参照してください。

Syntax
channel-group <slot/port>

<slot/port> - ポートチャネルのインタフェイス番号

初期設定

なし

コマンド･モード

インターフェイス･コンフィグ

コマンドの使用法

ポートチャネル 1 個あたりの最大メンバー数は 6 です。

9.4.10.12 **delete-channel-group**

このコマンドによりポートをポートチャネル (LAG) から削除します。インターフェイスは、設定ポートチャネルの論理スロット番号および論理ポート番号となります。

Syntax
delete-channel-group <slot/port>

<slot/port> - ポートチャネルのインタフェイス番号

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりすべての設定ポートをポートチャネル (LAG) から削除します。インターフェイスは、設定ポートチャネルの論理スロット番号および論理ポート番号となります。

Syntax
delete-channel-group <slot/port> all

<slot/port> - ポートチャネルのインタフェイス番号

all -特定のポートチャネルのすべてのメンバー

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.4.11 ストームの制御

9.4.11.1 show storm-control

このコマンドはブロードキャスト･ストームの制御情報を表示するために使われます。

Syntax
show storm-control broadcast

デフォルト設定

なし

コマンドモード

特権EXEC

メッセージを表示

Intf: インターフェイス番号を表示

Mode: ストーム制御ブロードキャストのステータスを表示

Level: ストーム制御ブロードキャストのレベルを表示

Rate: ストーム制御ブロードキャストのレートを表示

このコマンドはマルチキャスト･ストーム制御情報の表示に使われます。

Syntax
show storm-control multicast

デフォルトセッティング

なし

コマンドモード

特権EXEC

メッセージを表示

Intf: インターフェイス番号を表示.

Mode: ストーム制御マルチキャストのステータスを表示

Level: ストーム制御マルチキャストのレベルを表示

Rate: ストーム制御マルチキャストのレートを表示

このコマンドはユニキャスト･ストーム制御情報の表示に使われます。

Syntax
show storm-control unicast

デフォルトトセッティング

なし

コマンドモード

特権EXEC

メッセージを表示

Intf: インターフェイス番号を表示

Mode: ストーム制御ユニキャストのステータスを表示

Level: ストーム制御ユニキャストのレベルを表示

Rate: ストーム制御ユニキャストのレートを表示

9.4.11.2 storm-control broadcast

8 このコマンドは選択されたインターフェイスのブロードキャストストームリカバリーモードを有効化します。このモードが有効化されていると、高い閾値のブロードキャストストームリカバリーが実装されます。その閾値の実装はパーセンテージのパターンに従います。任意のイーサネットポートのブロードキャストのトラフィックがリンク速度の高い閾値(「ブロードキャストストームリカバリー閾値テーブル」に示されているように)のパーセンテージを超えるなら、スイッチはブロードキャストのトラフィックが閾値のパーセンテージかそれ以下へ戻るまではブロードキャストのトラフィックを破棄します。完全な実装については「ブロードキャストストームリカバリー閾値テーブル」に説明されています 。

Syntax
storm-control broadcast no storm-control broadcast

no -このコマンドは選択されたインターフェイスのブロードキャストストーム回復モードを無効化します。このモードが有効化されていると、高い閾値のブロードキャストストーム回復が実装されます。その閾値の実装はパーセンテージのパターンに従います。任意のイーサネットポートのブロードキャストのトラフィックがリンク速度の高い閾値(「ブロードキャストストーム回復閾値テーブル」に示されているように)のパーセンテージを超えるなら、スイッチはブロードキャストのトラフィックが閾値のパーセンテージかそれ以下へ戻るまではブロードキャストのトラフィックを破棄します。完全な実装については「ブロードキャストストーム回復閾値テーブル」に説明されています。

デフォルトトセッティング

無効

コマンドモード

インターフェイスの構成

このコマンドはすべてのインターフェイスのブロードキャストストームリカバリーモードを有効化します

Syntax
storm-control broadcast no storm-control broadcast

このコマンドはすべてのインターフェイスのブロードキャストストーム回復モードを無効化します。

デフォルトセッティング

無効

コマンドモード

グローバル・コンフィグ

9.4.11.3 **storm-control multicast**

このコマンドは選択されたインターフェイスのマルチキャストストーム回復モードを有効化します。

Syntax
storm-control multicast no storm-control multicast

no -このコマンドは選択されたインターフェイスのマルチキャストストームリカバリーモードを無効化します 。

デフォルトセッティング

なし

コマンドモード

インターフェイス･コンフィグ

このコマンドはすべてのインターフェイスのマルチキャストストームリカバリーモードを有効化します 。

Syntax
storm-control multicast no storm-control multicast

no -このコマンドはすべてのインターフェイスのマルチキャストストームリカバリーモードを無効化します 。

デフォルトセッティング

なし

コマンドモード

グローバル･コンフィグ

9.4.11.4 storm-control unicast

このコマンドは選択されたインターフェイスのユニキャスト･ストーム制御モードを有効化します。

Syntax
storm-control unicast no storm-control unicast

no - このコマンドは選択されたインターフェイスのユニキャスト･ストーム制御モードを無効化します。.

デフォルトセッティング

なし

コマンドモード

インターフェイス･コンフィグ

このコマンドはすべてのインターフェイスのユニキャスト･ストーム制御モードを有効化します。

Syntax
storm-control unicast no storm-control unicast

No - このコマンドはすべてのインターフェイスのユニキャスト･ストーム制御モードを無効化します。

デフォルトセッティング

なし

コマンドモード

グローバル･コンフィグ

9.4.11.5 switchport broadcast packet-rate

このコマンドは各ポートのブロードキャストトラフィックについての閾値レベルを設定することにより、ブロードキャストストームからネットワークを保護します 。

Syntax
switchport broadcast packet-rate {1 | 2 | 3 | 4}

1 - 閾値レベルは 64 pps (パケット毎秒)を表します。

2 - 閾値レベルは 128 pps (パケット毎秒)を表します。

3 - 閾値レベルは 256 pps (パケット毎秒)を表します。

4 - 閾値レベルは 516 pps (パケット毎秒)を表します。

デフォルトセッティング

レベル 4

コマンドモード

インターフェイス･コンフィグ

このコマンドはすべてのポートのブロードキャストトラフィックについての閾値レベルを設定することにより、ブロードキャストストームからネットワークを保護します 。

Syntax
switchport broadcast all packet-rate {1 | 2 | 3 | 4}

1 - 閾値レベルは 64 pps (パケット毎秒)を表します。

2 - 閾値レベルは 128 pps (パケット毎秒)を表します。

3 - 閾値レベルは 256 pps (パケット毎秒)を表します。

4 - 閾値レベルは 512 pps (パケット毎秒)を表します。

all - このコマンドはすべてのインターフェイスを表します。

デフォルトセッティング

レベル 4

コマンドモード

グローバル･コンフィグ

9.4.11.6 switchport multicast packet-rate

このコマンドは各ポートのマルチキャストトラフィックについての閾値レベルを設定することでマルチキャストストームからネットワークを保護します 。

Syntax
switchport multicast packet-rate {1 | 2 | 3 | 4}

1 - 閾値レベルは 64 pps (パケット毎秒)を表します。

2 - 閾値レベルは 128 pps (パケット毎秒)を表します。

3 - 閾値レベルは 256 pps (パケット毎秒)を表します。

4 - 閾値レベルは 516 pps (パケット毎秒)を表します。

デフォルトセッティング

レベル 4

コマンドモード

インターフェイス･コンフィグ

このコマンドはすべてのポートのマルチキャストトラフィックについての閾値レベルを設定することでマルチキャストストームからネットワークを保護します 。

Syntax
switchport multicast all packet-rate {1 | 2 | 3 | 4}

1 - 閾値レベルは 64 pps (パケット毎秒)を表します。

2 - 閾値レベルは 128 pps (パケット毎秒)を表します。

3 - 閾値レベルは 256 pps (パケット毎秒)を表します。

4 - 閾値レベルは 512 pps (パケット毎秒)を表します。

all - このコマンドはすべてのインターフェイスを表します。

デフォルトセッティング

レベル 4

コマンドモード

グローバル･コンフィグ

9.4.11.7 switchport unicast packet-rate

このコマンドは各ポートのユニキャストトラフィックについての閾値レベルを設定することでユニキャスト･ストームからネットワークを保護します 。

Syntax
switchport unicast packet-rate {1 | 2 | 3 | 4}

1 - 閾値レベルは 64 pps (パケット毎秒)を表します。

2 - 閾値レベルは 128 pps (パケット毎秒)を表します。

3 - 閾値レベルは 256 pps (パケット毎秒)を表します。

4 - 閾値レベルは 512 pps (パケット毎秒)を表します。

デフォルトセッティング

レベル 4

コマンドモード

インターフェイス･コンフィグ

このコマンドはすべてのポートのユニキャストトラフィックについての閾値レベルを設定することでユニキャスト･ストームからネットワークを保護します 。

Syntax
switchport unicast all packet-rate {1 | 2 | 3 | 4}

1 - 閾値レベルは 64 pps (パケット毎秒)を表します。

2 - 閾値レベルは 128 pps (パケット毎秒)を表します。

3 - 閾値レベルは 256 pps (パケット毎秒)を表します。

4 - 閾値レベルは 512 pps (パケット毎秒)を表します。

all - このコマンドはすべてのインターフェイスを表します。

デフォルトセッティング

レベル 4

コマンドモード

グローバル･コンフィグ

9.4.12 L2 プライオリティ

9.4.12.1 show queue cos-map

このコマンドにより特定のインターフェイスにおけるサービス優先度マップのクラスを表示します。

Syntax
show queue cos-map [<slot/port>]

<slot/port> - インターフェイス番号

初期設定

なし

コマンド･モード

特権EXEC

表示メッセージ

User Priority: マップされる 802.1pプライオリティを表示する。

Traffic Class: 該当する 802.1pプライオリティをマップする内部トラフィッククラスを示します。

9.4.12.2 **queue cos-map**

このコマンドによりCoS優先度キューにサービス (CoS) 値のクラスを割り当てます。

Syntax

queue cos-map <priority> <queue-id> no queue cos-map

<queue-id> - CoS優先度キューのキューID (範囲:0～7)

<priority> - キューIDにマップするCoS値 (範囲:0～7)

no - CoSマップをデフォルト値に戻します。

初期設定

プライオリティ	キュー
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

コマンド・モード

インターフェイス・コンフィグ

9.4.13 ポートミラー

9.4.13.1 show port-monitor session

このコマンドにより特定セッションのポート監視情報を表示します。

Syntax
show port-monitor session <SessionNum>

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Session ID: セッションIDを示します。

Admin Mode: ポート監視機能が有効であるか無効であるかを示します。 値はenabled またはdisabled となります。

Port: ターゲットポートとして設定されているスロット／ポート。この値が設定されていない場合は'Not Configured'と表示されます。

Port: ソースポートとして設定されているスロット／ポート。この値が設定されていない場合は'Not Configured'と表示されます。

9.4.13.2 port-monitor session

このコマンドにより監視セッション（ポート監視）にプローブポートおよび監視先ポートを設定します。ソースインターフェイスの<slot/port>パラメータを使用して、監視元のインターフェイスを指定します。受信パケットのみの監視にはrx、送信パケットのみの監視にはtxを使用します。{rx | tx}オプションを 指定して いない 場合、ターゲットポートで受信パケットと送信パケットの両方を監視します。ターゲットインターフェイスの<slot/port>パラメータを使用してインターフェイスを指定し、監視先のトラフィックを受信します。

Syntax
port-monitor session <session-id> {source interface <slot/port> [{rx | tx}] | destination interface <slot/port> } no port-monitor session <session-id> { source interface <slot/port> | destination interface <slot/port>}

<slot/port> - インターフェイス番号

tx/rx – 受信パケットまたは送信パケットを監視します。

no - このコマンドによりプローブポートまたはミラーポート を監視セッション （ポート監視）から削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドはすべての構成されたプローブポートとミラーポートを削除します。

Syntax
no port-monitor

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.4.13.3 port-monitor session mode

このコマンドにより監視セッションにおいてポート監視機能の管理モードを設定します。

Syntax
port-monitor session <session-id> mode no port-monitor session <session-id> mode

<session-id> - セッションID

no - このコマンドにより監視セッションについてポート監視機能を無効化します。

9.5 静的MACフィルタリングコマンド

9.5.1 コマンドを表示

9.5.1.1 show mac-addr-table static

このコマンドはすべての静的MACフィルタリング情報を表示します。<all>を使えばシステムのすべての静的MACフィルターが表示されます。<macaddr>の値を提供すると同時に<vlanid>の値も入力しなければなりません。そしてシステムはMACアドレスとVLANのみに静的MACフィルター情報を表示します 。

Syntax
show mac-addr-table static {<macaddr> <1-4094> | all}

<macaddr> -静的MACアドレス

デフォルトセッティング

なし

コマンド・モード

特権EXEC

メッセージを表示

MAC Address: 00:01:1A:B2:53:4Dの形式でのフィルターのMACアドレス.

VLAN ID: フィルターに関連付けられたVLAN ID

Source Port(s): 受信されたパケットをフィルタリングするために使うポートのリスト

9.5.2 構成コマンド

9.5.2.1 macfilter

このコマンドはVLAN<vlanid>上のMACアドレス<macaddr>のための静的MACエントリを作成します。<macaddr>パラメータの値は 6 バイトの 16 進数でB1:B2:B3:B4:B5:B6 の形式です。

制限されたMACアドレスは、00:00:00:00:00:00, 01:80:C2:00:00:00 から 01:80:C2:00:00:0F, 01:80:C2:00:00:20 から 01:80:C2:00:00:21, および FF:FF:FF:FF:FF:FF です。<vlanid> パラメータは有効なVLANを識別しなければなりません。20 までの静的MACフィルターを作ることができます。

Syntax
macfilter <macaddr> <1-4094> no macfilter <macaddr> <1-4094>

<macaddr> - B1:B2:B3:B4:B5:B6 の形式で 6 バイトの 16 進数を指定します。

no - このコマンドはVLAN上のMACアドレスへのすべてのフィルタリング制限と静的 MACフィルターの エントリを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.5.2.2 macfilter addsrc

このコマンドはMACアドレスとVLANと一緒にMACフィルターへ設定されたソースフィルターへインターフェイスを追加します。<macaddr>パラメータはB1:B2:B3:B4:B5:B6 の形式で 6 バイトの 16 進数で特定されなければなりません。<vlanid>パラメータは有効なVLANを識別しなければなりません。

Syntax
macfilter addsrc <macaddr> <1-4094> no macfilter addsrc <macaddr> <1-4094>

<macaddr> - B1:B2:B3:B4:B5:B6 の形式で 6 バイトの 16 進数により指定されています。

no - このコマンドはMACアドレスとVLANと一緒にMACフィルターへ設定されたソースフィルターからポートを削除します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ.

9.5.2.3 macfilter addsrc all

このコマンドはMACアドレスとVLANと一緒にMACフィルターへ設定されたソースフィルターへすべてのインターフェイスを追加します。<macaddr>パラメータはB1:B2:B3:B4:B5:B6 の形式で 6 バイトの 16 進数により指定します。<vlanid>パラメータは有効なVLANを識別しなければなりません。

Syntax
macfilter addsrc all <macaddr> <1-4094> no macfilter addsrc all <macaddr> <1-4094>

<macaddr> - B1:B2:B3:B4:B5:B6 の形式で 6 バイトの 16 進数で指定されています。

no - このコマンドはMACアドレスとVLANと一緒にMACフィルターへ設定されたソースフィルターからすべてのインターフェイスを削除します。

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.6 管理コマンド

9.6.1 ネットワークコマンド

9.6.1.1 show ip interface

このコマンドはスイッチのネットワークインターフェイスに関連付けられた構成設定を表示します。ネットワークインターフェイスはスイッチのフロントパネルポートのいずれかを経由したスイッチとのインバンドの接続に使われる論理的インターフェイスです。スイッチのネットワークインターフェイスに関連付けられた構成パラメータはトラフィックがスイッチイングまたはルーティングされるフロントパネルのポートの構成には影響を与えません。

Syntax
show ip interface

初期設定

なし

コマンド・モード

ユーザ EXEC, 特権EXEC

表示メッセージ

IP Address: インターフェイスのIPアドレス 工場側デフォルト設定値は 0.0.0.0 である。

netmask: インターフェイスのIPサブネットマスク。 工場側デフォルト設定値は 0.0.0.0 である。

VLAN: 管理VLAN IDを指定します。

9.6.1.2 show ip redirects

このコマンドはこのスイッチのIPデフォルトゲートウェイを表示します。

Syntax
show ip redirects

初期設定

なし

コマンド・モード

ユーザ EXEC, 特権EXEC

表示メッセージ

IP default gateway: IPインターフェイスのデフォルトゲートウェイ。工場側デフォルト設定値は 0.0.0.0 である。

9.6.1.3 show ip filter

このコマンドにより管理IPフィルターステータスおよびすべての指定管理ステーションを表示します。

Syntax
show ip filter

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Index: ステーション番号

IP Address: スイッチに構成の変更をすることが許可されたステーションのIPアドレス

9.6.1.4 mtu

このコマンドにより物理インターフェイスとポートチャネル (LAG) インターフェイスの最大送信単位 (MTU) のサイズ (バイト単位) を設定します。標準の実装では 1518～9216 の範囲の有効整数である<1518-9216>となります。

Syntax
mtu <1518-9216> no mtu

<1518-9216> -最大フレームサイズ (範囲: 1518 - 9216).

no - このコマンドによりインターフェイスのデフォルト最大送信単位 (MTU) のサイズ (バイト単位) を設定します。

初期設定

1518

コマンド・モード

インターフェイス・コンフィグ

9.6.1.5 interface vlan

このコマンドはインターフェイス-VLANコンフィグモードを入力するために使用されます。

Syntax
interface vlan <vlanid>

<vlanid> - VLAN ID(範囲 1～4094)

デフォルト設定

なし

コマンドモード

グローバル･コンフィグ

9.6.1.6 ip address

このコマンドによりIPアドレスおよびサブネットマスクを設定します。IPアドレスおよびゲートウェイは、同じサブネット上である必要があります。

Syntax
ip address <ipaddr> <netmask> no ip address

<ipaddr> - IP Address/IPアドレス

<netmask> - サブネットマスク

no - IPアドレスおよびサブネットマスクをデフォルト値に戻します。

初期設定

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

コマンド･モード

インターフェイス-VLANコンフィグ

コマンドの用法

IPアドレスを設定すると、VLAN IDの値が管理VLANに割り当てられます。

9.6.1.7 **ip default-gateway**

このコマンドによりデフォルトゲートウェイのIPアドレスを設定します。

Syntax
ip default-gateway <gateway> no ip default-gateway

< gateway > - デフォルトゲートウェイのIPアドレス

no - デフォルトゲートウェイのIPアドレスをデフォルト値に戻します。



インバンドおよびout-of-band (oob) の管理インターフェイスのゲートウェイを 一度に 設 定で きませ ん 。先にout-of-bandのゲートウェイ設定を行っている場合、 インバ ンド 管 理 インタ ーフェイスのゲートウェイ設定を行う前にそのout-of-bandのゲート ウェイ設 定を削 除する必 要 があります。

初期設定

IP Address: 0.0.0.0

コマンド・モード

グローバル・コンフィグ

9.6.1.8 **ip address protocol**

このコマンドにより使用するネットワーク設定プロトコルを指定します。この値を変更すると、その変更内容が即時に適用されます。

Syntax
ip address protocol {bootp | dhcp | none}

<bootp> - BOOTPからIPアドレスを取得します。

<dhcp> - DHCPからIPアドレスを取得します。

<none> - 設定を行い、IPアドレスを取得します。



インバンドおよびout-of-bandの管理インターフェイス両方で、DHCPを使用して 一度に IP アドレスをDHCPサーバから取得するよう設定できます。ただし、 同時に取得 できま せん。

初期設定

なし

コマンド・モード

インターフェイス-VLANコンフィグ

9.6.1.9 enable ip filter

このコマンドによりIPフィルタ機能を有効化します。

Syntax
ip filter no ip filter

no – IPフィルタ機能を無効化します。

初期設定

無効

コマンド･モード

グローバル･コンフィグ

9.6.1.10 ip filter

このコマンドによりIPアドレスのフィルタ設定を行います。

Syntax
ip filter <ipaddr> no ip filter <ipaddr>

<ipaddr> - フィルタ設定を行うIPアドレスを設定します。

no -設定したフィルタIPアドレスを削除します。

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.6.1.11 show oob

このコマンドにより (OOB) インターフェイスに関連する設定を表示します。

Syntax
show oob

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

IP Address: インターフェイスのIPアドレス 工場側デフォルト設定値は 0.0.0.0 である。

Subnet Mask: インターフェイスのIPサブネットマスク。 工場側デフォルト設定値は 0.0.0.0 である。

Default Gateway: ゲートウェイのIPアドレス.

IPv6 Address: OOBインターフェイスのIPv6 アドレス

OOB interface Configured Protocol: 使用するネットワーク設定プロトコル。 デフォルト設定はDHCPである。

Burned In MAC Address: OOBインターフェイスのデフォルトMACアドレス

9.6.1.12 oob ip

このコマンドによりIPアドレス、およびoobインターフェイスのサブネットマスクを設定します。IPアドレスおよびゲートウェイは、同じサブネット上である必要があります。

Syntax
oob ip <ipaddr> <netmask>

<ipaddr> - IP Address/IPアドレス

<netmask> - サブネットマスク

初期設定

IP Address: 0.0.0.0

サブネットマスク : 0.0.0.0

コマンド・モード

グローバル・コンフィグ

9.6.1.13 **oob gateway**

このコマンドはout-of-bandインターフェイスのデフォルトゲートウェイのIPアドレスを設定します。

Syntax
oob gateway <gateway> no oob gateway

< gateway > - デフォルトゲートウェイのIPアドレス

no - デフォルトゲートウェイのIPアドレスをデフォルト値に戻します。



インバンドおよびout-of-band (oob) の管理インターフェイスのゲートウェイを一度に 設定できません。先にout-of-bandのゲートウェイ設定を行っている場合、インバンド管 理インターフェイスのゲートウェイ設定を行う前にそのout-of-bandのゲートウェイ設定を 削除す る必要があります。

初期設定

Gateway Address : 0.0.0.0

コマンド・モード

グローバル・コンフィグ

9.6.1.14 **oob protocol**

このコマンドにより使用するoob設定プロトコルを指定します。この値を変更すると、その変更内容が即時に適用されます。

Syntax
oob protocol {bootp | dhcp | dhcp6 | none}

<bootp> - BOOTPからIPアドレスを取得します。

<dhcp> - DHCPからIPアドレスを取得します。

<dhcp6> - IPv6 アドレスをDHCPv6 から取得します。

<none> - 設定を行い、IPアドレスを取得します。



インバンドおよびout-of-bandの管理インターフェイス両方で、DHCPを使用して一度に IP アドレスをDHCPサーバから取得するよう設定できます。ただし、同時に取得できません。

初期設定

DHCP

コマンド・モード

グローバル・コンフィグ

9.6.2 シリアルインターフェイスコマンド

9.6.2.1 show line console

このコマンドはスイッチへのシリアル通信の設定を表示します。

Syntax
show line console

初期設定

なし

コマンド・モード

ユーザ EXEC, 特権EXEC

表示メッセージ

Serial Port Login Timeout (minutes): スイッチが接続を切った後のシリアルポート接続での稼働停止の時間を分で指定します。0 から 160 の数字での任意の値を使えます。工場デフォルト値は 5 です。0 の値はタイムアウトを無効化します。

Baud Rate: シリアルポートが接続を試行するボーレートのデフォルト値。使用できる値は 1200、2400、4800、9600、19200、38400、57600、115200 ボーです。

Character Size: 一文字のビット数。 ビット数はつねに 8 となります。

Flow Control: ハードウェアフロー制御が有効であるか無効であるかを示します。ハードウェアフロー制御はつねに無効化されます。

Stop Bits: 一一文字毎のストップビット数。 ストップビットは 1 です。

Parity: シリアルポートで使用されるパリティーの方法。 パリティーメソッドは常にNoneです。

Password Threshold: インバンドTelnetセッションの管理モード この値を無効化に設定するとTelnetポートを遮断する。 管理モードが無効化されていると、すべての既存のTelnet接続が切断される。 デフォルト値は有効である。

Silent Time (sec): パスワード閾値コマンドにより設定された閾値を失敗したログオン試行回数が超過した後、管理コンソールにアクセス不能になるまでの時間をこのコマンドで設定する。

9.6.2.2 line console

このコマンドにより行設定モードに入ります。

Syntax
line console

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.6.2.3 baudrate

このコマンドにより端末インターフェイスの通信速度を指定します。サポートされる速度は 1200、2400、4800、9600、19200、38400、57600、115200 です。

Syntax
baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200} no baudrate

no - このコマンドにより端末インターフェイスの通信速度を 9600 に設定します。

初期設定

9600

コマンド・モード

ラインコンフィグ

9.6.2.4 exec-timeout

このコマンドによりコンソール最大無動作接続時間 (分単位) を指定します。0 の値は、コンソールが無期限に接続できることを示します。時間の範囲は 0～160 分です。

Syntax
exec-timeout <0-160>

<0-160> -最大接続時間 (範囲:0～160)

no - このコマンドによりコンソール最大無動作接続時間 (分単位) を 5 に設定します。

初期設定

5

コマンド・モード

ラインコンフィグ

9.6.2.5 password-threshold

このコマンドによりパスワード不正によるログイン失敗時の、パスワード入力制限数を設定します。

Syntax
password-threshold <0-120> no password-threshold

<threshold> -最大閾値 (範囲：0～120)

no - このコマンドにより最大値をデフォルト値に設定します。

初期設定

3

コマンド・モード

ラインコンフィグ

9.6.2.6 silent-time

このコマンドにより所定回数以上ログインに失敗した場合に管理コンソールがアクセス不可となる時間を設定します。

Syntax
silent-time <0-65535>

<0-65535> -秒単位のサイレント時間(範囲： 0 - 65535) in seconds.

no - このコマンドにより最大値をデフォルト値に設定します。

初期設定

0

コマンド・モード

ラインコンフィグ

9.6.2.7 login local

このコマンドによりログイン時のパスワード確認を有効化します。

Syntax
login local

初期設定

無効化

コマンド・モード

ラインコンフィグ

9.6.2.8 terminal-length

このコマンドによりCLIコンソール端末の長さを設定します。

Syntax
terminal-length <10-100> no terminal-length

<length> -最大閾値(範囲： 10 - 100).

no - このコマンドにより長さをデフォルト値に設定します。

初期設定

24

コマンド・モード

ラインコンフィグ

9.6.2.9 show pager

このコマンドによりページャー設定を表示します。

Syntax
show pager

初期設定

なし

コマンド・モード

特権EXEC

9.6.2.10 pager

このコマンドによりペイジャーモードを有効化／無効化します。ページャーモードが有効の場合、データは端末上で 1 ページに表示されます。

Syntax
pager no pager

no - このコマンドによりページャーモードを無効に設定します。

初期設定

有効化

コマンド・モード

特権EXEC

9.6.2.11 show displaymode

このコマンドにより拡張表示設定を表示します。

Syntax
show displaymode

初期設定

なし

コマンド・モード

特権EXEC

9.6.2.12 displaymode

このコマンドにより拡張表示モードを有効／無効化します。拡張表示モードで、1 行あたり 80 文字以上の情報が表示されます。

Syntax
displaymode no displaymode

no - このコマンドにより拡張表示モードを無効に設定します。

i	拡張表示モードで情報を正しく表示するには、1 行あたり 80 文字以上の表示に対応した端末を使用する必要があります。

初期設定

有効化

コマンド・モード

特権EXEC

9.6.3 Telnetセッションコマンド

9.6.3.1 telnet

このコマンドによりリモートホストへの新規アウトバウンドtelnet接続を作成します。

Syntax
telnet <host> [port] [debug] [line] [echo]

<host> - ホスト名または有効なIPアドレス

[port] - 0～65535 の範囲の有効な 10 進法の整数。デフォルト値は 23

[debug] - 現在有効となっているtelnetオプションを表示します。

[line] - アウトバウンドtelnet動作モードをlinemodeに設定します。デフォルトの動作モードはcharacter modeです。

[echo] - ローカルエコーを有効化します。

初期設定

なし

コマンド・モード

ユーザ EXEC, 特権EXEC

9.6.3.2 show line vty

このコマンドによりtelnetの設定を表示します。

Syntax
show line vty

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Remote Connection Login Timeout (minutes): ログオフ前にリモート接続セッションが動作停止する時間を分単位で示します。ゼロはタイムアウトがないことを示します。0～160 の数を指定できます。デフォルト値は 5 である。

Maximum Number of Remote Connection Sessions: 許可される同時リモート接続セッション数を示します。 デフォルト値は 5 である。

Allow New Telnet Sessions: noに設定されている場合、新規telnetセッションが許可されないことを示します。デフォルト値はyesです。

Password Threshold: ログオン試行の回数限度にコンソール・ポートで到達すると、システム・インターフェイスは次のログオン試行を許可するまでは所定時間応答を止める。 (silent time コマンドでこの間隔を設定する。) Telnetでこの閾値に到達するとTelnetのログオン・インターフェイスは閉じる。

9.6.3.3 line vty

このコマンドによりvty (Telnet) 設定モードに入ります。

Syntax
line vty

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.6.3.4 server enable

このコマンドによりtelnetサーバを有効または無効化します。

Syntax
server enable no server enable

no - このコマンドで無効に設定します。

初期設定

有効化

コマンド・モード

Line Vty

9.6.3.5 exec-timeout

このコマンドによりリモート接続セッションタイムアウトの値を分単位で設定します。設定した時間中にセッションがアイドル状態であれば、そのセッションはアクティブとなります。0 の値はセッションが無期限にアクティブとなることを示します。時間は 0～160 の 10 進法の値です。

Syntax
exec-timeout <1-160> no exec-timeout

<sec> -最大接続時間(範囲： 1 -160).

no - このコマンドによりリモート接続セッションタイムアウトの分単位の値をデフォルト値に設定します。



アクティブセッションのタイムアウト値の変更は、そのセッションに再度アクセスすると適用されます。または、いずれかのキーを押すと新しいタイムアウト値が適用されます。

初期設定

5

コマンド・モード

Line Vty

9.6.3.6 password-threshold

このコマンドによりパスワード不正によるログイン失敗時の、パスワード入力制限数を設定します。

Syntax
password-threshold <0-120> no password-threshold

<threshold> -最大閾値(範囲： 0 - 120).

no - このコマンドにより最大値をデフォルト値に設定します。

初期設定

3

コマンド・モード

Line Vty

9.6.3.7 maxsessions

このコマンドにより確立できるリモート接続セッションの最大数を指定します。0 の値は、リモート接続が確立できないことを示します。範囲は 0〜5 です。

Syntax
maxsessions <0-5> no maxsessions

<0-5> -最大セッション数(範囲： 0 - 5).

no - このコマンドにより最大値を 5 に設定します。

初期設定

5

コマンド・モード

Line Vty

9.6.3.8 sessions

このコマンドにより新規telnetセッションを調整します。セッションが有効の場合、使用可能なセッションがそれ以上ない場合に新規telnetセッションを確立できます。セッションが無効の場合、新規telnetセッションを確立できません。確立したセッションは、終了するまで、または異常ネットワークエラーにより終了されるまでアクティブとなります。

Syntax
sessions no sessions

no - このコマンドによりtelnetセッションを無効化します。セッションが無効の場合、新規telnetセッションを確立できません。

初期設定

有効

コマンド・モード

Line Vty

9.6.3.9 terminal-length

このコマンドによりCLI VTP端末の長さを設定します 。

Syntax
terminal-length <10-100> no terminal-length

<length> -最大閾値(範囲: 10 - 100).

no - このコマンドにより長さをデフォルト値に設定します。

初期設定

24

コマンド・モード

Line Vty

9.6.3.10 telnet sessions

このコマンドにより新規アウトバウンドtelnet接続を調整します。有効の場合、新規アウトバウンドtelnetセッションは、許可される同時アウトバウンドtelnetセッションの最大数に到達するまで確立できます。無効の場合、新規アウトバウンドtelnetセッションを確立できません。確立したセッションは、終了するまで、または異常ネットワークエラーにより終了されるまでアクティブとなります。

Syntax
telnet sessions no telnet sessions

no - このコマンドにより新規アウトバウンドtelnet接続を無効化します。無効の場合、新規アウトバウンドtelnet接続を確立できません。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

9.6.3.11 telnet maxsessions

このコマンドにより同時アウトバウンドtelnetセッションの最大数を指定します。0 の値は、アウトバウンドtelnetセッションを確立できないことを示します。

Syntax
telnet maxsessions <0-5> no maxsessions

<0-5> -最大セッション数(範囲： 0 - 5).

no - このコマンドにより最大値を 5 に設定します。

初期設定

5

コマンド・モード

グローバル・コンフィグ

9.6.3.12 **telnet exec-timeout**

このコマンドによりアウトバウンドtelnetセッションのタイムアウト値を分単位で設定します。

Syntax
telnet exec-timeout <1-160> no telnet exec-timeout

<1-160> -最大接続時間(範囲： 1 -160).

no - このコマンドにより分単位のリモート接続セッションのタイムアウト値をデフォルト値に設定します。



アクティブセッションのタイムアウト値の変更は、そのセッションに再度アクセスすると適用されます。または、いずれかのキーを押すと新しいタイムアウト値が適用されます。

初期設定

5

コマンド・モード

グローバル・コンフィグ

9.6.3.13 **show telnet**

このコマンドにより現在のアウトバウンドtelnet設定を表示します。

Syntax
show telnet

初期設定

なし

コマンド・モード

ユーザ EXEC, 特権EXEC

表示メッセージ

Outbound Telnet Login Timeout (in minutes): ログオフするまでアウトバンドtelnetセッションが動作停止となる分単位の時間を示します。0 の値はデフォルト値であり、タイムアウトにならないことを示します。

Maximum Number of Outbound Telnet Sessions: 許可される同時アウトバウンドtelnet接続数を示します。

Allow New Outbound Telnet Sessions: アウトバウンドtelnetセッションを許可するかを示します。

9.6.4 SNMPサーバコマンド

9.6.4.1 show snmp

このコマンドによりSNMPコミュニティー情報を表示します。

6 個のコミュニティーがサポートされます。コミュニティーの追加、変更、削除ができます。有効化するためにスイッチをリセットする必要はありません。

スイッチのSNMPエージェントはSNMPバージョン 1、2c、 及び、3 (SNMPの規格について詳しくはSNMP RFCを参照)に従っています。SNMPエージェントはSNMP構成(トラップレシーバーと他のSNMPコミュニティーのパラメータ)に基づいて外部のSNMPマネージャへTCP/IPを通してトラップを送ります。

Syntax
show snmp

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

SNMP Community Name: エントリがアクセスを許可するコミュニティー名。有効なエントリは、大文字と小文字で区別される最大 16 文字の英数字です。テーブルの各列には固有のコミュニティー名を付ける必要があります。

Client IP Address: デバイスが関連コミュニティーのSNMPパケットを受信するIPアドレス (またはその一部) 。要求エンティティのIPアドレスは、そのIPアドレスとの比較前にサブネットマスクとANDされます。注記：サブネットマスクが 0.0.0.0 に設定されている場合、0.0.0.0 のIPアドレスはすべてのIPアドレスと一致します。デフォルト値は 0.0.0.0 です。

Client IP Mask: IPアドレスとの比較前に要求エンティティのIPアドレスとANDされるマスク。結果がIPアドレスと一致すると、そのアドレスは認証済みIPアドレスとなります。例えば、IPアドレスが 9.47.128.0、対応サブネットマスクが 255.255.255.0 の場合、受信IPアドレスの範囲が一致します。つまり、受信IPアドレスは 9.47.128.0 - 9.47.128.255 と同等となります。デフォルト値は 0.0.0.0 です。

Access Mode: コミュニティー文字列のアクセスレベル

Status： コミュニティーアクセスエントリのステータス

9.6.4.2 show trapflags

このコマンドはトラップの条件を表示します。トラップ条件を有効化または無効化することでどのトラップが作成されるべ

きかを構成します。トラップ条件が有効で条件が検出されれば、スイッチのSNMPエージェントはすべての有効なトラップレシーバーへトラップを送ります。スイッチは変更を実装するためにリセットされる必要はありません。コールドとウォームスタートのトラップが常に作成され、無効化できません。

Syntax
show trapflags

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Authentication Flag: 有効化または無効化します。 デフォルト設定は有効化されている。認証失敗トラップを送信するかを示します。

Link Up/Down Flag: 有効化または無効化します。 デフォルト設定は有効化されている。リンクステータストラップを送信するかを示します。

Multiple Users Flag: 有効化または無効化が可能。工場デフォルト設定値は有効化。同じユーザーIDが同時に一回以上(Telnet かシリアルポート経由で)スイッチへログインしたときはトラップが送られるか否かを示します。

Spanning Tree Flag: 有効化または無効化が可能。工場デフォルト設定値は有効化。スパニングツリーのトラップが送られるか否かを示します。

ACL Traps: 有効化または無効化します。 工場側デフォルトは無効化されている。 ACLトラップを送信するかを示します。

9.6.4.3 snmp-server sysname

このコマンドはスイッチの名前を設定します。名前の範囲は 1～31 字の英数字です。

Syntax
snmp-server sysname <name>

<name> -名前の範囲は 1～31 文字の英数字です。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.6.4.4 snmp-server location

このコマンドはスイッチの物理的場所を設定します。名前の範囲は 1～31 字の英数字です。

Syntax
snmp-server location <loc>

<loc> - 名前の範囲は 1～31 文字の英数字です。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.6.4.5 snmp-server contact

このコマンドによりネットワーク管理装置を設定します。範囲は 1～31 文字の英数字です 。

Syntax
snmp-server contact <con>

<con> - 名前の範囲は 1～31 文字の英数字です。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.6.4.6 snmp-server community

このコマンドは新しいSNMPコミュニティーを追加(そして名前付け)します。コミュニティーの名前はスイッチに関連付けられると同時に特定の特権レベルで管理する一群のSNMPマネージャに関連付けられた名前です。名前の長さは大文字小文字を区別する 16 文字までです。

注記: SNMPコミュニティーテーブルのコミュニティー名は固有のものであ る必要があります。 同じコミュ ニティー名を使用し複数のエントリを作成した場合、最初のエントリが保持および処理され、その他の重複エントリは無視されます。

Syntax
snmp-server community <name> no snmp-server community <name>

<name> - コミュニティー名 (大文字と小文字で区別される最大 16 文字)

no – このコマンドによりこのコミュニティー名をテーブルから削除します。 名前は削除するコミュ ニティー名となります。

初期設定

publicおよびprivateの 2 つのデフォルトコミュニティー名。このデフォルトコミュニティー名を、コミュニティーごとに固有の識別子に変更できます。残りの 4 つのコミュニティー名のデフォルト値は空欄となっています。

コマンド・モード

グローバル・コンフィグ

このコマンドはSNMPコミュニティーを有効化します。コミュニティーが有効化されると、このコミュニティーマネージャに関連付けられたSNMPマネージャはそのアクセス権に従ってスイッチを管理します。コミュニティーが無効化されると、このコミュニティーを使用するSNMPの要求は受け入れられません。この場合このコミュニティーに関連付けられたSNMPマネージャはステータスが有効化されるまでスイッチを管理できません。

Syntax
snmp-server community mode <name> no snmp-server community mode <name>

<name> - コミュニティー名

no - このコマンドはSNMPコミュニティーを無効化します。コミュニティーが無効にされればこのコ ミュニティーによるSNMPの要求は受け入れられません。この場合コミュニティーに関連付けられたSNMPマネージャはステータスが有効化されるまでスイッチを管理できません。

初期設定

publicおよびprivateのコミュニティーはデフォルトで有効化されています。また、定義されていない 4 つのコミュニティーはデフォルトで無効化されています。

コマンド･モード

グローバル･コンフィグ

このコマンドによりSNMPコミュニティーにクライアントIPマスクを設定します。アドレスは、関連コミュニティーのSNMPパケット送信アドレスであり、デバイスへのアクセス時にSNMPクライアントがコミュニティーを使用できるIPアドレスの範囲を示す、クライアントIPアドレスの値とともに使用されます。255.255.255.255 の値で 1 ステーションからのアクセスを許可し、クライアントIPアドレスのマシンIPアドレスを使用します。0.0.0.0 の値ですべてのIPアドレスからのアクセスを許可します。名前は、該当するコミュニティー名となります。

Syntax
snmp-server community ipmask <ipmask> <name> no snmp-server community ipmask <name>

<name> - コミュニティー名

<ipmask> - クライアントIPマスク

no - このコマンドによりSNMPコミュニティーのクライアントIPマスクを 0.0.0.0 に設定します。 名前は、該当するコミュニティー名となります。コミュニティー名には最大 16 文字の英数字を使用できます。

初期設定

0.0.0.0

コマンド･モード

グローバル･コンフィグ

このコマンドはスイッチ情報へのアクセスを制限します。アクセスモードは読み取り専用(パブリックとも呼ばれる)または Read･Write可(プライベートとも呼ばれる)です。

Syntax
snmp-server community {ro | rw} <name>

<name> - コミュニティー名

<ro> - アクセスモードは読み取り専用

<rw> - アクセスモードはRead･Write可

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.6.4.7 snmp-server host

このコマンドによりSNMPコミュニティーのクライアントIPアドレスを設定します。アドレスは、関連コミュニティーのSNMPパケット送信アドレスであり、デバイスへのアクセス時にSNMPクライアントがコミュニティーを使用できるIPアドレスの範囲を示す、クライアントIPマスク値とともに使用されます。0.0.0.0 の値ですべてのIPアドレスからのアクセスを許可します。クライアントIPアドレスのマシンIPアドレスを使用します。0.0.0.0 の値ですべてのIPアドレスからのアクセスを許可します。それ以外の場合、この値はマスクとANDされ、許可するクライアントIPアドレスの範囲が決定されます。名前は、該当するコミュニティー名となります。

Syntax
snmp-server host <ipaddr> <name> No snmp-server host <name>

<name> - コミュニティー名

<ipaddr> - クライアントIPアドレス

no - このコマンドによりSNMPコミュニティーのクライアントIPアドレスを 0.0.0.0 に設定します。 名前は、該当するコミュニティー名となります。

初期設定

0.0.0.0

コマンド・モード

グローバル・コンフィグ

9.6.4.8 snmp-server enable traps

このコマンドによりACLトラップを有効化します。

Syntax
snmp-server enable traps acl-trapflags no snmp-server enable traps acl-trapflags

no - このコマンドによりACLトラップを無効化します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

このコマンドにより認証トラップを有効化します。

Syntax
snmp-server enable traps authentication no snmp-server enable traps authentication

no - このコマンドにより認証トラップを無効化します。

初期設定

有効

コマンド･モード

グローバル･コンフィグ

このコマンドはスイッチ全体のリンクアップ/リンクダウンのトラップを有効化します。有効化された場合、リンクトラップはポートに関連付けられたリンクトラップフラッグが有効化されている場合のみリンクトラップが送られます。('snmp trap link-status'コマンドを参照)

Syntax
snmp-server enable traps linkmode no snmp-server enable traps linkmode

no - このコマンドはスイッチ全体のリンクアップ/リンクダウンのトラップを無効化します。

初期設定

有効

コマンド･モード

グローバル･コンフィグ

このコマンドによりMultiple Userトラップを有効化します。トラップが有効の場合、およびユーザーが端末インターフェイス (EIA 232 またはtelnet) にログインし、現在端末インターフェイスセッションがある場合に、Multiple Userトラップが送信されます。

Syntax
snmp-server enable traps multiusers no snmp-server enable traps multiusers

no - このコマンドによりMultiple Userトラップを無効化します。

初期設定

有効

コマンド･モード

グローバル･コンフィグ

このコマンドは新しいルートトラップとトポロジー変更通知トラップの送信を有効化します。

Syntax
snmp-server enable traps stpmode no snmp-server enable traps stpmode

no - このコマンドは新しいルートトラップとトポロジー変更通知トラップの送信を有効化します。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

9.6.5 SNMPトラップコマンド

9.6.5.1 show snmptrap

このコマンドはSNMPトラップレシーバーを表示します。トラップメッセージはネットワークでSNMPネットワークマネージャへ送られます。これらのメッセージはスイッチまたはネットワーク内部で起こっているイベントをマネージャに通知します。6 個のトラップレシーバーが同時にサポートされています。

Syntax
show snmptrap

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

SNMP Trap Name: トラップマネージャへ送信されるSNMPトラップパケットのコミュニティー名。最大 16 文字の英数字を使用できます。文字列は大文字、小文字で区別されます。

IP Address: SNMPトラップをデバイスから受信するIPアドレス。0 から 255 までの 4 個の数字をピリオドで区切り入力する。

SNMP Version: レシーバーが使用するトラップバージョン

SNMP v1 - SNMP v1 を使用し、レシーバーへトラップを送信

SNMP v2 - SNMP v2 を使用し、レシーバーへトラップを送信

Status: レシーバーのステータス (有効または無効) を示し、管理者／ユーザーによるこのユーザーエントリへの動作を許可するプルダウンメニュー

Enable - レシーバーへトラップを送信する

Disable - レシーバーへトラップを送信しない

9.6.5.2 **snmp trap link-status**

このコマンドによりインターフェイスのリンクステータストラップを有効化します。

注記:このコマンドはLink Up/Downフラグが有効な場合のみ、有効化されます。**snmp-server enable traps linkmode**コマンドを参照してください。

Syntax
snmp trap link-status no snmp trap link-status

no - このコマンドによりインターフェイスのリンクステータストラップを無効化します。

初期設定

無効化

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりすべてのインターフェイスのリンクステータストラップを有効化します。

注記: このコマンドはLink Up/Downフラグが有効な場合のみ、有効化されます (**snmp-server enable traps linkmode**コマンドを参照してください) 。

Syntax
snmp trap link-status all no snmp trap link-status all

all - すべてのインターフェイス。

no - このコマンドによりすべてのインターフェイスのリンクステータストラップを無効化します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

9.6.5.3 snmptrap <name> <ipaddr>

このコマンドによりSNMPトラップ名を追加します。名前は大文字と小文字で区別される最大 16 文字の英数字です。

Syntax
snmptrap <name> <ipaddr> no snmptrap <name> <ipaddr>

<name> - SNMPトラップ名 (範囲：大文字と小文字で区別される最大 16 文字の英数字)

<ipaddr> - トラップレシーバーのIPアドレス

no - このコマンドでコミュニティーのトラップレシーバーを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.6.5.4 snmptrap ipaddr

このコマンドにより特定コミュニティー名のトラップレシーバーのIPアドレスを変更します。名前は大文字と小文字で区別される最大 16 文字の英数字です。.

注記：SNMPトラップレシーバーテーブルのIPアドレスは、同じコミュニティー名で固有のものである必要があります。同じIPアドレスおよびコミュニティー名を使用し複数のエントリを作成した場合、最初のエントリが保持および処理され、その他の重複エントリは無視されます。

Syntax
snmptrap ipaddr <name> <ipaddr> <ipaddrnew>

<name> - SNMPトラップ名

<ipaddr> - 元のIPアドレス

<ipaddrnew> - 新規IPアドレス

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.6.5.5 snmptrap mode

このコマンドによりSNMPトラップをアクティブ化または非アクティブ化します。有効なトラップレシーバーはアクティブ化され（トラップ受信可）、無効なトラップレシーバーは非アクティブ化され（トラップ受信不可）ます。

Syntax

```
snmptrap mode <name> <ipaddr>
no snmptrap mode <name> <ipaddr>
```

<name> - SNMPトラップ名

<ipadd> - IPアドレス

no - このコマンドによりSNMPトラップを非アクティブ化します。トラップレシーバーは非アクティブ化します（トラップを受信できません）。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

8.1.1.1 snmptrap snmpversion

このコマンドによりSNMPトラップをアクティブ化または非アクティブ化します。有効なトラップレシーバーはアクティブ化され（トラップ受信可）、無効なトラップレシーバーは非アクティブ化され（トラップ受信不可）ます。

Syntax

```
snmptrap snmpversion <name> <ipaddr> <snmpv1|snmpv2>
```

<name> - SNMPトラップ名

<ipadd> - IPアドレス

snmpv1 - SNMP v1 を使用し、トラップを送信

Snmpv2 - SNMP v3 を使用し、トラップを送信

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.6.6 HTTPコマンド

9.6.6.1 show ip http

このコマンドはスイッチのhttp設定を表示します。

Syntax
show ip http

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

HTTP Mode (Unsecure): HTTPモードが有効であるか無効であるかを示します。

HTTP Port: HTTPに設定されているポートを示します。

HTTP Mode (Secure): セキュアHTTPの管理モードが有効であるか無効であるかを示します。

Secure Port: セキュアHTTPに設定されているポートを示します。

Secure Protocol Level(s): プロトコルレベルはSSL3、TSL1、またはSSL3 とTSL1 両方のいずれかの値となります。

9.6.6.2 ip javamode

このコマンドはウェブのインターフェイスのヘッダーフレームでJavaアプレットへのアクセスをスイッチが許可すべきかどうかを指定します。アクセスが有効化されていると、Javaアプレットはウェブインターフェイスから見ることができます。無効化された場合、ユーザーはJavaアプレットを見ることは出来ません。

Syntax
ip javamode no ip javamode

no - このコマンドはウェブインターフェイスのヘッダーフレームにあるJavaアプレットへのアクセスを非許可します。Javaモードが無効化された場合、ユーザーはJavaアプレットを見ることは出来ません。

初期設定

有効化

コマンド・モード

グローバル・コンフィグ

9.6.6.3 ip http port

このコマンドによりhttpポートを 1-65535 に設定します。デフォルトのポートは 80 です。

Syntax
ip http port <1-65535> no ip http port

<1-65535> - HTTPポート値

no - このコマンドによりhttpポートをデフォルト値にリセットします。

初期設定

80

コマンド・モード

グローバル・コンフィグ

9.6.6.4 ip http server

このコマンドはウェブインターフェイス経由でスイッチへのアクセスを有効化します。アクセスが有効化されていると、ユーザーはウェブインターフェイスからスイッチへログインできます。無効化された場合、ユーザーはスイッチのウェブサーバへログインできません。

Webインターフェイスを無効にすると即時にすべてのインターフェイスに適用されます。

Syntax
ip http server no ip http server

no - このコマンドはウェブインターフェイス経由でスイッチへのアクセスを有効化します。アクセスが無効化された場合、ユーザーはスイッチのウェブサーバへログインできません。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

9.6.6.5 ip http secure-port

このコマンドによりセキュアHTTPポートを 1-65535 に設定します。デフォルトのポートは 443 です。

Syntax
ip http secure-port <portid> no ip http secure-port

<portid> - セキュアHTTPポート値

no - このコマンドによりセキュアHTTPポートをデフォルト値にリセットします。

初期設定

443

コマンド･モード

グローバル･コンフィグ

9.6.6.6 ip http secure-server

このコマンドによりセキュアHTTPのセキュアソケットレイヤーを有効化します。

Syntax
ip http secure-server no ip http secure-server

no - このコマンドによりセキュアHTTPのセキュアソケットレイヤーを無効化します。

初期設定

無効

コマンド･モード

グローバル･コンフィグ

9.6.6.7 ip http secure-protocol

このコマンドによりプロトコルレベル (バージョン) を設定します。プロトコルレベルはTLS1、SSL3、またはTLS1 とSSL3 両方のいずれかに設定できます。

Syntax
ip http secure-protocol <protocollevel1> [protocollevel2] no ip http secure-protocol <protocollevel1> [protocollevel2]

<protocollevel1 - 2> - プロトコルレベルはTLS1、SSL3、またはTLS1 とSSL3 両方のいずれかに設定できます。

no - このコマンドによりセキュアHTTPのプロトコルレベル (バージョン) を削除します。

初期設定

SSL3 とTLS1

コマンド・モード

グローバル・コンフィグ

9.6.6.8 ip http session

このコマンドによりhttp hard-timeout、maxsessions、およびsoft-timeoutのパラメータを設定します。

Syntax
ip http session { hard-timeout <0-168> | maxsessions <0-16> | soft-timeout <0-60> } no ip http session { hard-timeout | maxsessions | soft-timeout }

hard-timeout <0-168>: HTTPセッションのハードタイムアウト (時間単位) を設定します。

maxsessions <0-16>: HTTPセッションの最大許可数を設定します。

soft-timeout <0-60>: HTTPセッションのソフトタイムアウト (分単位) を設定します。

no - このコマンドによりHTTPセッションのパラメータをデフォルト値に戻します。

初期設定

maxsessions: 16

hard-timeout: 24

soft-timeout: 15

コマンド・モード

グローバル・コンフィグ

9.6.6.9 ip http secure-session

このコマンドによりhttp hard-timeout、maxsessions、およびsoft-timeoutのパラメータを設定します。

Syntax
ip http secure-session { hard-timeout <0-168> | maxsessions <0-16> | soft-timeout <0-60> } no ip http secure-session { hard-timeout | maxsessions | soft-timeout }

hard-timeout <0-168>: セキュアHTTPセッションのハードタイムアウト (時間単位) を設定します。

maxsessions <0-16>: セキュアHTTPセッションの最大許可数を設定します。

soft-timeout <0-60>: セキュアHTTPセッションのソフトタイムアウト (分単位) を設定します。

no - このコマンドによりセキュアHTTPセッションのパラメータをデフォルト値に戻します。

初期設定

maxsessions: 16

hard-timeout: 24

soft-timeout: 5

コマンド・モード

グローバル・コンフィグ

9.6.7 セキュアShell (SSH) コマンド

9.6.7.1 show ip ssh

このコマンドによりSSH設定を表示します。

Syntax
show ip ssh

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Administrative Mode: SSHの管理モードが有効であるか無効であるかを示します。

Protocol Levels: プロトコルレベルはversion 1、version 2、あるいは両方のバージョンとなります。

SSH Sessions Currently Active: 現在のSSH接続数を示します。

Max SSH Sessions Allowed：スイッチに許可されるインバウンドの最大SSHセッション数。

SSH Timeout：この欄はスイッチへの着信SSHセッションに対する無動作タイムアウト値です。

9.6.7.2 ip ssh

このコマンドによりSSH設定を表示します。

Syntax
ip ssh no ip ssh

no - このコマンドによりSSHを無効化します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

9.6.7.3 ip ssh protocol

このコマンドによりSSHのプロトコルレベル (またはバージョン) を設定または削除します。SSH1 (1)、SSH2 (2)、あるいはSSH 1 とSSH 2 (1 and 2) 両方のいずれかに設定できます。

Syntax
ip ssh protocol <protocollevel1> [protocollevel2]

<protocollevel1 - 2> - プロトコルレベルはSSH1、SSH2、あるいはSSH 1 とSSH 2 両方のいずれかに設定できます。

初期設定

SSH1 と SSH2

コマンド・モード

グローバル・コンフィグ

9.6.7.4 ip ssh maxsessions

このコマンドにより作成できるSSH接続セッションの最大数を指定します。0 の値はssh接続を作成できないことを示します。範囲は 0～5 です。

Syntax
ip ssh maxsessions <0-5> no ip ssh maxsessions

<0-5> - セッションの最大数

no - このコマンドにより作成できるSSH接続セッションの最大数をデフォルト値に戻します。

初期設定

5

コマンド・モード

グローバル・コンフィグ

9.6.7.5 **ip ssh timeout**

このコマンドによりSSH接続セッションタイムアウト値を分単位で設定します。セッションが指定時間中アイドル状態であれば、そのセッションはアクティブとなります。0 の値はセッションが無期限にアクティブとなることを示します。時間の整数値の範囲は 0～160 です。アクティブセッションのタイムアウト値の変更は、そのセッションに再度アクセスすると適用されます。または、いずれかのキーを押すと新しいタイムアウト値が適用されます。

Syntax

```
ip ssh timeout <1-160>
no ip ssh timeout
```

<1-160> -秒単位のタイムアウト間隔

no - このコマンドにより分単位のSSH接続セッションタイムアウト値をデフォルト値に戻します。 アクティブセッションのタイムアウト値の変更は、そのセッションに再度アクセスすると適用されます。または、いずれかのキーを押すと新しいタイムアウト値が適用されます。

初期設定

5

コマンド・モード

グローバル・コンフィグ

9.6.8 DHCPクライアントコマンド

9.6.8.1 ip dhcp restart

このコマンドによりBOOTPまたはDHCPのクライアント要求を開始します。

Syntax
ip dhcp restart

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.6.8.2 ip dhcp client-identifier

このコマンドはこのスイッチに対するDHCPクライアント識別子を指定するために使用されます。デフォルト値に戻すにはno ip dhcp client-identifierを使用します 。

Syntax
ip dhcp client-identifier {text <text> | hex <hex>} no ip dhcp client-identifier

<text> - テキスト文字列(範囲: 1-15 characters).

<hex> - XX:XX:XX:XX:XX:XX (Xは 0～9、A～F) 形式の 16 進数文字列

no - このコマンドによりデフォルト値に戻ります。



接続ブレードのMMBまたはCLIからホスト名が変更されると、DHCPクライアント識別子も変更されます。

初期設定

CB.SerialNumber

コマンド・モード

グローバル・コンフィグ

9.6.9 DHCPv6 クライアントコマンド

9.6.9.1 ipv6 address protocol

このコマンドにより使用するIPv6 設定プロトコルのネットワークを指定します。この値を変更すると、その変更内容が即時に適用されます。

Syntax
ipv6 address protocol {dhcp6 | none}

<dhcp6> - DHCPv6 からIPアドレスを取得します。

<none> - 設定を行い、IPアドレスを取得します。

初期設定

なし.

コマンド・モード

インターフェイス-VLANコンフィグ

9.6.9.2 ipv6 dhcp6 restart

このコマンドによりネットワークインターフェイスからのDHCPv6 クライアント要求を開始します。

Syntax
ipv6 dhcp6 restart

初期設定

なし.

コマンド・モード

グローバル・コンフィグ

9.6.9.3 oob protocol

このコマンドにより使用するoob設定プロトコルを指定します。この値を変更すると、その変更内容が即時に適用されます。

Syntax
oob protocol {bootp | dhcp | dhcp6 | none}

<bootp> - BOOTPからIPアドレスを取得します。

<dhcp> - DHCPからIPアドレスを取得します。

<dhcp6> - IPv6 アドレスをDHCPv6 から取得します。

<none> - 設定を行い、IPアドレスを取得します。

初期設定

DHCP.

コマンド・モード

グローバル・コンフィグ

9.6.9.4 oob protocol dhcp6 restart

このコマンドによりoobインターフェイスからのDHCPv6 クライアント要求を開始します。

Syntax
oob protocol dhcp6 restart

初期設定

なし.

コマンド・モード

グローバル・コンフィグ

9.6.10 ドメインネームサーバリレーコマンド

9.6.10.1 Showコマンド

9.6.10.1.1 show hosts

このコマンドにより静的ホストのネーム-アドレスマッピングテーブルを表示します 。

Syntax
show hosts

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Domain Name List: ドメイン名

IP Address: ホストのIPアドレス

9.6.10.1.2 show dns

このコマンドによりDNSサーバの設定を表示します。

Syntax
show dns

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

サーバ名：DDNSのプロバイダー名。

Default Domain Name: ホストのIPアドレスのクエリに使用するデフォルトのドメイン名

Domain Name List: ホストのIPアドレスのクエリに使用するドメイン名のリスト

Name Server List: ドメインネームサーバのリスト

Request: 送信されたDNSクエリパケットの数

Response: 受信されたDNS応答パケットの数

9.6.10.2 show dns cache

このコマンドによりDNSキャッシュテーブルにあるすべてのエントリを表示します。

Syntax
show dns cache

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Domain Name List: ドメイン名

IP Address: 該当するドメイン名のIPアドレス

TTL: このエントリがDNSキャッシュテーブルに保持される秒単位の時間

Flag: このエントリの信頼性を示します。8 の値は 10 の値より信頼性はありません。

9.6.10.3 設定コマンド

9.6.10.3.1 ip hosts

このコマンドによりIPアドレスにホスト名をマップするDNSテーブルに、静的エントリを作成します。

Syntax
ip host <name> <ipaddr> no ip host <name>

<name> - ホスト名

<ipaddr> - ホストのIPアドレス

<no> - IPアドレスのマッピングエントリから該当する名前を削除します。

初期設定

なし

コマンド・モード

特権EXEC

9.6.10.3.2 clear hosts

このコマンドにより静的ホスト全体のname-to-addressマッピングテーブルをクリアします。

Syntax
clear hosts

初期設定

なし

コマンド･モード

特権EXEC

9.6.10.3.3 ip domain-name

このコマンドにより不完全なホスト名（クライアントから送信されたホスト名に「.」が使用されていない場合）に付与するデフォルトのドメイン名を定義します。

Syntax
ip domain-name <name> no ip domain-name <name>

<name> - 未認定のホスト名を完了させるために使用されるデフォルト･ドメイン名 未認定の名前をドメイン名から分離する初期フェーズは含めないこと。 (範囲: 1-64 文字)

初期設定

なし

コマンド･モード

特権EXEC

9.6.10.3.4 ip domain-list

このコマンドにより不完全なホスト名（クライアントから送信されたホスト名に「.」が使用されていない場合）に付与するドメイン名を定義します。ドメイン名テーブルには最大 6 エントリを含めることができます。

Syntax
ip domain-list <name> no ip domain-list <name>

<name> - 未認定のホスト名を完了させるために使用されるデフォルト・ドメイン名 未認定の名前をドメイン名から分離する初期フェーズは含めないこと。 (範囲: 1-64 文字)



不完全なホスト名がスイッチのDNSサーバで受信されたとき、それはドメイン名リストを検索し、リストの各ドメイン名をそのホスト名に追加し特定のネームサーバが一致するかどうかをチェックします。ドメイン名リストがない場合は、「ip domain-name」コマンドで特定されたドメイン 名が使われます。ドメイン名リストがあれば、デフォルトドメイン名が使われます。

初期設定

なし

コマンド・モード

特権EXEC

9.6.10.3.5 ip name-server

このコマンドによりネーム-アドレス解決に使用する複数のドメインネームサーバのアドレスを指定 します。ドメインネームサーバテーブルには最大 6 エントリを含めることができます 。

Syntax
ip name-server <ipaddr> no ip name-server <ipaddr>

< ipaddr > - ドメインネームサーバのIPアドレス

<no> -該当するドメインネームサーバエントリをテーブルから削除します。



列記されたネームサーバは、応答を受信するまで、あるいはリストの最後まで応答がない場合に、指定シーケンスでクエリされます。

初期設定

なし

コマンド・モード

特権EXEC

9.6.10.3.6 ip domain-lookup

このコマンドによりIPドメインネームシステム (DNS) ベースのホストのネーム-アドレス変換を有効化します 。

Syntax
ip domain-lookup no ip domain-lookup

<no> - このコマンドによりIPドメインネームシステム (DNS) ベースのホストのname-to-address変換を無効化します。

初期設定

なし

コマンド・モード

特権EXEC

9.6.10.3.7 clear domain-list

このコマンドによりドメイン名リストテーブルのすべてのエントリをクリアします。

Syntax
clear domain-list

初期設定

なし

コマンド・モード

特権EXEC

9.6.10.3.8 clear dns

このコマンドによりDNSをデフォルト値に戻します。

Syntax
clear dns

初期設定

なし

コマンド・モード

特権EXEC

9.6.10.3.9 clear dns cache

このコマンドによりDNSキャッシュテーブルのすべてのエントリをクリアします。

Syntax
clear dns cache

初期設定

なし

コマンド・モード

特権EXEC

9.6.10.3.10 clear dns counter

このコマンドによりDNSキャッシュテーブルのすべてのエントリの統計データをクリアします。

Syntax
clear dns cache

初期設定

なし

コマンド・モード

特権EXEC

9.6.11 動的DNSクライアントコマンド

9.6.11.1 ddns client

このコマンドによりddnsプロバイダがドメインレコードを更新したことを通知するためのDDNS (動的DNS) 更新を行います。更新が成功した場合、ddnsリストにそのパラメータが保存されます。

動的DNSは、IPルータやコンピュータシステムなどのインターネットプロトコルスイートを使用しネットワーク上のデバイスに機能を提供する、メソッド、プロトコル、あるいはネットワークサービスです。設定ホスト名、アドレス、またはDNSに保存されているその他の情報のアクティブDNS設定の変更について、ドメインネームサーバへリアルタイムに通知を行います。

Syntax
ddns { dhs | dyndns | dyns | easydns | ods | tzo | zoneedit } <username> <password> <host> [<address>] no ddns { dhs | dyndns | dyns | easydns | ods | tzo | zoneedit } <username> <password> <host> [<address>]

<no> - このコマンドによりddns設定をリストから削除します。

初期設定

なし.

コマンド・モード

グローバル・コンフィグ

9.6.11.2 show ddns

このコマンドによりDDNS設定リストを表示します。

Syntax
Show ddns

初期設定

なし.

コマンド・モード

特権EXEC

表示メッセージ

Server Name: DDNSサーバのプロバイダ名

User Name: DDNSサーバのユーザー名

Password: アカウントのパスワード

Host: IPアドレスでマップするドメイン名

IP Address: ドメイン名でマップするIPアドレス

9.6.12 IPv6 コマンド

9.6.12.1 show ipv6 interface

このコマンドによりIBPのIPv6 ネットワーク設定を表示します。

Syntax
show ipv6 interface

初期設定

なし.

コマンド・モード

ユーザ EXEC, 特権EXEC

表示メッセージ

IPv6 Address: インターフェイスのIPv6 アドレス

Address mode: 使用するIPv6 プロトコルのネットワーク設定。デフォルト値はNone.

9.6.12.2 show ipv6 traffic

このコマンドによりIPv6 と ICMPv6 のトラフィックおよび統計データを表示します。 インターフェイスを指定し、その トラフィック情報を閲覧できます 。

Syntax
show ipv6 traffic {oob | switchport}

初期設定

なし.

コマンド・モード

ユーザ EXEC, 特権EXEC

表示メッセージ

Total Datagrams Received: インターフェイスで受信した、エラーを含む入力データグラムの合計数

Received Datagrams Locally Delivered: IPv6 ユーザープロトコル (ICMPを含む) に正しく送信されたデータグラムの合計数。このカウンタはこのデータグラムが宛てられたインターフェイスでインクリメントします。データグラムによっては入力インターフェイスとは限りません。

Received Datagrams Discarded Due To Header Errors: バージョン番号不一致、その他の形式エラー、ホップカウント超過、IPv6 オプション処理中のエラー検出などを含むIPv6 ヘッダーのエラーにより破棄された、入力データグラムの数。

Received Datagrams Discarded Due To MTU: サイズが送信インターフェイスのリンクMTUのサイズを超過した

ため送信できなかった、入力データグラムの数。

Received Datagrams Discarded Due To No Route: 宛先に送信するルートが見つからなかったため破棄された、入力データグラムの数。

Received Datagrams With Unknown Protocol: 正しく受信したが、不明または非対応プロトコルのため破棄された、ローカルでアドレスされたデータグラムの数。このカウンタはこのデータグラムが宛てられたインターフェイスでインクリメントします。データグラムによっては入力インターフェイスとは限りません。

Received Datagrams Discarded Due To Invalid Address: IPv6 ヘッダーの宛先フィールドのIPv6 アドレスが、このエンティティで受信できる有効アドレスでないため破棄された、入力データグラムの数。このカウントには、無効なアドレス (::0 など) や非対応アドレス (割り当てられていないアドレスなど) が含まれます。IPv6 ルーターではないためデータグラムを転送しないエンティティについては、このカウンターはターゲット・アドレスがローカル・アドレスでなかったために破棄されたデータグラムを含む 。

Received Datagrams Discarded Due To Truncated Data: データグラムフレームに十分なデータがないため破棄された、入力データグラムの数。

Received Datagrams Discarded Other: 継続的処理に問題は無かったが破棄された(たとえばバッファー容量不足等)入力されたIPv6 データダイアグラムの数。このカウンターは再構築を待っているあいだに破棄されたデータダイアグラムは含まないことを注記しておきます 。

Received Datagrams Reassembly Required: インターフェイスで再取得する必要のあるIPv6 フラグメント数。注記：このカウンタはこのフラグメントが宛てられたインターフェイスでインクリメントします。フラグメントの入力インターフェイスとは限りません 。

Datagrams Successfully Reassembled: 正しく再取得されたIPv6 データグラムの数。注記：このカウンタはこのデータグラムが宛てられたインターフェイスでインクリメントします。フラグメントの入力インターフェイスとは限りません。

Datagrams Failed To Reassemble: IPv6 再取得アルゴリズムで検出された失敗数 (タイムアウト、エラーなど、すべての理由による) 。注記：受信時に結合されているアルゴリズム (受信アルゴリズム) もあるため、破棄されたIPv6 フラグメント数とは限りません。このカウンタはフラグメントが宛てられたインターフェイスでインクリメントします。フラグメントの入力インターフェイスとは限りません 。

Datagrams Forwarded: エンティティがターゲットで送受信した出力データグラムの数。IPv6 ルータとして動作しないエンティティ内では、このカウンタにはこのエンティティを経由しソースルートされたパケットのみが含まれ、ソースルート処理は成功となります。注記：データグラムの転送が成功すると、出力インターフェイスのカウンタがインクリメントします。

Datagrams Locally Transmitted: 送信要求でローカルIPv6 ユーザープロトコル (ICMPを含む) によりIPv6 に送信されたIPv6 データグラムの合計数。注記：このカウンタにはipv6IfStatsOutForwDatagramsのデータグラムは含まれません。

Datagrams Transmit Failed: 宛先へ送信できない問題は存在しないが破棄された (バッファスペース不足など) 出力IPv6 データグラムの数。注記：パケットがこの (任意の) 破棄規則に該当する場合、このカウンタにはipv6IfStatsOutForwDatagramsのデータグラムは含まれません。

Fragments Created: 出力インターフェイスのフラグメントにより作成された出力データグラムフラグメント数 。

Datagrams Successfully Fragmented: 出力インターフェイスで正しくフラグメントされたIPv6 データグラムの数 。

Datagrams Failed To Fragment: 出力インターフェイスでフラグメントする必要があるが失敗したため破棄されたIPv6 データグラムの数

Multicast Datagrams Received: インターフェイスで受信したマルチキャストパケットの数。

Multicast Datagrams Transmitted: インターフェイスが送信されたマルチキャストパケットの数。

合計受信ICMPv6 メッセージ：ipv6IfIcmpInErrorsでカウントされた数を含む、インターフェイスで受信したICMPメ

ッセージの合計数。注記：このインターフェイスは、ICMPメッセージが宛てられたインターフェイスであり、メッセージの入力インターフェイスであるとは限りません。

ICMPv6 Messages with errors: インターフェイスで受信しICMPの特定エラー（ICMPチェックサム、不正な長さなど）により与えられたICMPメッセージの数。

ICMPv6 Destination Unreachable Messages: インターフェイスで受信したICMP Destination Unreachableメッセージの数。

ICMPv6 Messages Prohibited Administratively: インターフェイスで受信した、管理者に禁止されるICMP destination unreachable/communicationメッセージの数。

ICMPv6 Time Exceeded Messages: インターフェイスで受信したICMP Time Exceededメッセージの数。

ICMPv6 Parameter Problem Messages: インターフェイスで受信したICMP Parameter Problemメッセージの数。

ICMPv6 messages with too big packets: インターフェイスで受信したICMP Packet Too Bigメッセージの数。

ICMPv6 Echo Request Messages Received: インターフェイスで受信したICMP Echo（要求）メッセージの数。

ICMPv6 Echo Reply Messages Received: インターフェイスで受信したICMP Echo Replyメッセージの数。

ICMPv6 Router Solicit Messages Received: インターフェイスで受信したICMP Router Solicitメッセージの数。

ICMPv6 Router Advertisement Messages Received: インターフェイスで受信したICMP Router Advertisementメッセージの数。

ICMPv6 Neighbor Solicit Messages Received: インターフェイスで受信したICMP Neighbor Solicitメッセージの数。

ICMPv6 Neighbor Advertisement Messages Received: インターフェイスで受信したICMP Neighbor Advertisementメッセージの数。

ICMPv6 Redirect Messages Received: インターフェイスで受信したRedirectメッセージの数。

ICMPv6 Group Membership Query Messages Received: インターフェイスで受信したICMPv6 Group Membership Queryメッセージの数。

ICMPv6 Group Membership Response Messages Received: インターフェイスで受信したICMPv6 group Membership Responseメッセージの数。

ICMPv6 Group Membership Reduction Messages Received: インターフェイスで受信したICMPv6 Group Membership Reductionメッセージの数。

Total ICMPv6 Messages Transmitted: インターフェイスが送信試行したICMPメッセージの合計数。注記：このカウンタにはicmpOutErrorsでカウントされたすべての数が含まれます。

ICMPv6 Messages Not Transmitted Due To Error: ICMPでバッファ不足などの問題がありインターフェイスが送信しなかったICMPメッセージの数。この値には、IPv6 が結果データグラムをルートできないなどのICMPレイヤー外で検出されたエラーは含まれません。実装によってはこのカウンタ値に該当するエラータイプがない場合があります。

ICMPv6 Destination Unreachable Messages Transmitted: インターフェイスが送信したICMP Destination Unreachableメッセージの数。

ICMPv6 Messages Prohibited Administratively Transmitted: インターフェイスが送信した、管理者に禁止されるICMP destination unreachable/communicationメッセージの数。

ICMPv6 Time Exceeded Messages Transmitted: インターフェイスが送信したICMP Time Exceededメッセージの数。

ICMPv6 Parameter Problem Messages Transmitted: インターフェイスが送信したICMP Parameter Problemメッセージの数。

ICMPv6 Packet Too Big Messages Transmitted: インターフェイスが送信したICMP Packet Too Bigメッセージの数。

ICMPv6 Echo Request Messages Transmitted: インターフェイスが送信したICMP Echo (要求) メッセージの数。

ICMPv6 Echo Reply Messages Transmitted: インターフェイスが送信したICMP Echo Replyメッセージの数。

ICMPv6 Router Solicit Messages Transmitted: インターフェイスが送信したICMP Router Solicitationメッセージの数。

ICMPv6 Router Advertisement Messages Transmitted: インターフェイスで受信したICMP Router Advertisementメッセージの数。

ICMPv6 Neighbor Solicit Messages Transmitted: インターフェイスが送信したICMP Neighbor Solicitationメッセージの数。

ICMPv6 Neighbor Advertisement Messages Transmitted: インターフェイスが送信したICMP Neighbor Advertisementメッセージの数。

ICMPv6 Redirect Messages Transmitted: インターフェイスが送信したRedirectメッセージの数。ホストはRedirectを送信しないため、ホストでこのオブジェクトはつねにゼロとなります。

ICMPv6 Group Membership Query Messages Transmitted: インターフェイスが送信したICMPv6 Group Membership Queryメッセージの数。

ICMPv6 Group Membership Response Messages Transmitted: インターフェイスが送信したICMPv6 group Membership Responseメッセージの数。

ICMPv6 Group Membership Reduction Messages Transmitted: インターフェイスが送信したICMPv6 Group Membership Reductionメッセージの数。

ICMPv6 Duplicate Address Detects: インターフェイスが検出した重複アドレスの数。

9.6.12.3 clear ipv6 statistics

このコマンドにより特定インターフェイスのIPv6 統計データをクリアします。show ipv6 trafficコマンドの出力でIPv6 統計データを表示します。

Syntax
clear ipv6 statistics {oob | switchport}

初期設定

なし.

コマンド・モード

特権EXEC

9.6.13 CDP コマンド

9.6.13.1 show cdp

このコマンドはCDP構成情報を表示します。

Syntax
show cdp

デフォルトトセッティング

なし

コマンドモード

特権EXEC

メッセージを表示

CDP Admin Mode: CDPが有効化または無効化.

CDP Hold Time (sec): 受信デバイスがL2 ネットワークスイッチのCDP情報を、破棄するまでに保 持すべき時 間の長さ

CDP Transmit Interval (sec): CDPパケットを送るためのL2 ネットワークスイッチの時間

Port: ポート番号 対 CDPステータス

CDP: CDPが有効化か無効化

9.6.13.2 show cdp neighbors

このコマンドはCDP周辺の情報を保持します。.

Syntax
show cdp neighbors

デフォルトトセッティング

なし

コマンドモード

特権EXEC

メッセージを表示

Device Id: 文字列形式でデバイス名を識別します。

Local Interface: CDP周辺情報を受信するポート。

Holdtime: 受信デバイスが、破棄するまでにCDP情報を保持すべき時間の長さ

Capability: デバイスタイプの形式、たとえばスイッチ等でのデバイスの機能性を解説します。

Platform: デバイスのハードウェアプラットフォーム、たとえばFSC the L2 ネットワークスイッチを解説します。

Port Id: CDPパケットが送られるポートを識別します。

9.6.13.3 show cdp traffic

このコマンドはCDPトラフィックカウンター情報を表示します。

Syntax
show cdp traffic

デフォルトセッティング

なし

コマンドモード

特権EXEC

メッセージを表示

Incoming packet number: 周辺から受信した正常なCDPパケット番号

Outgoing packet number: このデバイスから送信されたCDPパケット番号

Error packet number: 周辺から受信した異常CDPパケットの番号

9.6.13.4 cdp

9 このコマンドはCDP管理モードを有効化するために使われます。

Syntax
cdp no cdp

no – このコマンドはCDP管理モードを無効化するために使われます。

デフォルトセッティング

有効化

コマンドモード

グローバル·コンフィグ

9.6.13.5 cdp run

10 このコマンドは指定されたインターフェイスでCDPを有効化するために使用します。

Syntax
cdp run no cdp run

no – このコマンドは特定のインターフェイス上のCDPを無効化するために使われます。

デフォルトセッティング

有効化

コマンドモード

インターフェイスの構成

このコマンドはすべてのインターフェイスでCDPを有効化するために使われます。

Syntax
cdp run all no cdp run all

all - すべてのインターフェイス。

no – このコマンドはすべてのインターフェイスのCDPを無効化するために使われます。

デフォルトセッティング

有効化

コマンドモード

グローバル･コンフィグ

9.6.13.6 cdp timer

このコマンドは送信CDPパケットの間隔(秒) を構成するために使用されます。

Syntax
cdp timer <5-254> no cdp timer

<5-254> -間隔時間(範囲　5～254)

no - このコマンドは間隔時間をデフォルト値に戻します。

デフォルトセッティング

60

コマンドモード

グローバル･コンフィグ

9.6.13.7 cdp holdtime

このコマンドはCDPの保持時間(秒数)を構成するために使われます。

Syntax
cdp holdtime <10-255>

<10-255> - 間隔時間(範囲　10～255)

No – このコマンドは保持時間をデフォルト値に保持するために使われます。

デフォルトセッティング

180

コマンドモード

グローバル･コンフィグ

9.6.14 LLDPコマンド

9.6.14.1 show lldp

このコマンドにより現在のLLDP設定の概要を表示します。

Syntax

```
show lldp
```

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Transmit Interval: システムがローカルデータLLDPフレームを送信する間隔を秒単位で示します。

Transmit Hold Multiplier: ローカルデータLLDPフレームにTTLを設定する送信間隔のマルチプライヤを示します。

Re-initialization Delay: 再開までの遅延時間を秒単位で示します。

Notification Interval: システムがリモートデータ変更通知を送信する間隔を秒単位で示します。

9.6.14.2 show lldp interface

このコマンドにより特定インターフェイスまたはすべてのインターフェイスの現在のLLDP設定の概要を表示します。

Syntax

```
show lldp interface {<slot/port> | all}
```

<slot/port> -特定のインターフェイスを構成する。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Interface：インターフェイスをスロット／ポートの表記で示します。

Link: リンクがupであるかdownであるかを示します。

Transmit: インターフェイスがLLDPフレームを送信するかを示します。

Receive: インターフェイスがLLDPフレームを受信するかを示します。

Notify: インターフェイスがリモートデータ変更通知を送信するかを示します。

TLVs: インターフェイスがLLDPフレームに任意のTLVを送信するかを示します。TLVコードは 0 (ポート記述) 、1 (システム名) 、2 (システム記述) 、3 (システム機能) のいずれかとなります。

Mgmt: インターフェイスがLLDPフレームにシステム管理アドレス情報を送信するかを示します。

9.6.14.3 show lldp statistics

このコマンドにより特定インターフェイスまたはすべてのインターフェイスの現在のLLDPトラフィックおよびリモートテーブル統計データを表示します。

Syntax
show lldp statistics {<slot/port> | all}

<slot/port> -特定のインターフェイスを構成する。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Last Update: リモートテーブルへの最終更新からの経過時間を日、時間、分、秒で示します。

Total Inserts: リモートデータテーブルへの挿入の合計数

Total Deletes: リモートデータテーブルからの削除の合計数

Total Drops: 受信した完全なリモートデータが不正リソースのため挿入されなかった合計回数

Total Ageouts: TTL間隔が期限切れのため完全なリモートデータエントリが削除された合計回数

テーブルには以下の行見出しが表示されます。

Interface：インターフェイスをスロット／ポートの表記で示します。

Transmit Total: ポートに送信されたLLDPフレームの合計数

Receive Total: ポートで受信したLLDPフレームの合計数

Discards: なんらかの理由によりポートで破棄されたLLDPフレームの合計数

Errors: ポートで受信した無効LLDPフレーム数

Ageouts: Time to Live intervalが期限切れのためポートで完全なリモートデータが削除された合計回数

TLV Discards: 破棄されたTLV数

TLV Unknowns: タイプ値が制限範囲内のため認識されなかった場合の、ポートで受信したLLDP TLVの合計数

9.6.14.4 show lldp remote-device

このコマンドにより現在のLLDPデータをシステムに送信するリモートデバイスの概要情報を表示します。すべてのポートまたは特定のポートで受信したLLDPリモートデータの情報を表示できます。

Syntax
show lldp remote-device {<slot/port> | all}

<slot/port> -特定のインターフェイスを示します。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Local Interface: リモートデバイスからLLDPフレームを受信したインターフェイスを示します。

Chassis ID: リモートデバイスのIDを示します。

Port ID: LLDPフレームを送信したポート番号を示します。

System Name: リモートデバイスのシステム名を示します。

9.6.14.5 show lldp remote-device detail

このコマンドにより現在のLLDPデータをシステムのインターフェイスに送信するリモートデバイスに関する詳細情報を表示します。

Syntax
show lldp remote-device detail <slot/port>

<slot/port> -特定のインターフェイスを示します。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Local Interface: リモートデバイスからLLDPフレームを受信したインターフェイスを示します。

Chassis ID Subtype: Chassis IDフィールドで使用されている認識タイプを示します。

Chassis ID: リモートデバイスのシャーシを示します。

Port ID Subtype: リモートデバイスのポートタイプを示します。

Port ID: LLDPフレームを送信したポート番号を表示します。

System Name: リモートデバイスのシステム名を示します。

System Description: システム名、およびデバイスでサポートされているハードウェア、OS、ネ ットワークソフトウェアのバージョンを識別し、リモートシステムを記述します。

Port Description: 英数字でポートを記述します。ポート記述は設定可能です。

System Capabilities Supported: デバイスのプライマリ機能を示します。

System Capabilities Enabled: 有効である対応システム機能を示します。

Management Address: LLDPエージェントのあるリモートデバイスの各インターフェイ スで、リモートLLDPエージェントが使用するアドレスタイプを列記し、デバイスに関連する情報を取得するアドレスを指定します。

Time To Live: LLDPフレームで受信したリモートデバイスの情報を有効な情報として 処理するまでの時間（秒単位）を示します。

9.6.14.6 show lldp local-device

このコマンドにより通知されたLLDPローカルデータに関する概要情報を表示します。各インターフェイスの概要情報または詳細情報を表示できます。

Syntax
show lldp local-device {<slot/port> | all}

<slot/port> - 特定のインターフェイスを示します。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Interface：インターフェイスをスロット／ポートの表記で示します。

Port ID: インターフェイスに関連するポートIDを示します。

Port Description: インターフェイスに関連するポート記述を示します。

9.6.14.7 show lldp local-device detail

このコマンドにより特定のインターフェイスが送信するLLDPデータの詳細情報を表示します。

Syntax
show lldp local-device detail <slot/port>

<slot/port> - 特定のインターフェイスを示します。

初期設定

なし

コマンド･モード

特権EXEC

表示メッセージ

Interface:LLDPフレームを送信するインターフェイスを示します。

Chassis ID Subtype: Chassis IDフィールドで使用されている認識タイプを示します。

Chassis ID: ローカルデバイスのシャーシを示します。

Port ID Subtype: ローカルデバイスのポートタイプを示します。

Port ID: LLDPフレームを送信したポート番号を示します。

System Name: ローカルデバイスのシステム名を示します。

System Description: システム名、およびデバイスでサポートされているハードウェア、OS、ネットワークソフトウェアのバージョンを識別し、ローカルシステムを記述します。

Port Description: 英数字でポートを記述します。

System Capabilities Supported: デバイスのプライマリ機能を示します。

System Capabilities Enabled: 有効である対応システム機能を示します。

Management Address: ローカルLLDPエージェントが情報の送受信に使用するアドレスタイプおよび特定のアドレスを列記します。

9.6.14.8 lldp notification

このコマンドによりリモートデータ変更通知を有効化します。

Syntax
lldp notification no lldp notification

no - このコマンドにより通知を無効化します。

初期設定

無効

コマンド・モード

インターフェイス・コンフィグ

9.6.14.9 lldp notification-interval

このコマンドによりシステムがリモートデータ変更通知を送信する間隔を設定します。<interval-seconds>パラメータは、通知送信ごとの秒単位の待機時間です。有効な間隔範囲は 5～3600 秒です。

Syntax
lldp notification-interval <interval-seconds> no lldp notification-interval

<interval-seconds> -通知送信ごとの待機時間を秒単位で設定します。

no - このコマンドにより通知間隔をデフォルト値に戻します。

初期設定

5

コマンド・モード

グローバル・コンフィグ

9.6.14.10 lldp receive

このコマンドによりLLDP受信機能を有効化します。

Syntax

```
lldp receive
no lldp receive
```

no - このコマンドによりLLDPフレームの受信機能をデフォルト値に戻します。

初期設定

無効化

コマンド・モード

インターフェイス・コンフィグ

9.6.14.11 lldp transmit

このコマンドによりLLDPアドバタイズ機能を有効化します。

Syntax

```
lldp transmit
no lldp transmit
```

no - このコマンドによりローカルデータ送信機能をデフォルト値に戻します。

初期設定

無効化

コマンド・モード

インターフェイス・コンフィグ

9.6.14.12 lldp transmit-mgmt

このコマンドはローカルシステム管理アドレス情報の送信をLLDPフレームに含めるために使われます。

Syntax

```
lldp transmit-mgmt
no lldp transmit-mgmt
```

no - このコマンドによりLLDPフレームへの管理情報の追加をキャンセルします。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

9.6.14.13 **lldp transmit-tlv**

このコマンドによりLLDPフレームに送信する 802.1AB基本管理設定の任意のタイプの長さの値 (TLV) を指定します。sys-nameを使用すると、 システム名のTLVを送信します。 システム名の設定方法 につ い て は 、snmp-serverコマンドを参照してください。sys-desctoを使用すると、システム記 述のTLV を送信します。sys-capを使用すると、システム機能のTLVを送信します。port-descを使用 すると、 ポート記述のTLVを送信します。ポート記述の設定方法については、descriptionコマンドにより参照してください。

Syntax
lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc] no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]

no - このコマンドにより任意のTLVをLLDPフレームから削除します。 パラメータのないコマンドを 使用すると、 すべての任意のTLVをLLDPフレームから削除します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

9.6.14.14 **lldp timers**

このコマンドによりLLDPが有効であるポートのローカルデータ送信のタイミングパラメータを設定します。<interval-seconds>で、ローカルデータLLDPフレームの送信ごとの待機時間を 秒単位で設 定しま す。範囲は 1〜32768 秒です。<hold-value>は、ローカルデータLLDPフレームのTTLを設定す る送信 間 隔 のマルチプライヤを示し、範囲は 2〜10 です。<reinit-seconds>は、再開までの遅延時間を示し、範囲は 1〜0 秒です。

Syntax
lldp timers [interval <interval-seconds>] [hold <hold-value>] [reinit <reinit-seconds>] no lldp timers [interval] [hold] [reinit]

<interval-seconds> - ローカルデータLLDPフレームの送信ごとの待機時間を秒単位で設定します。

<hold-value> - ローカルデータLLDPフレームにTTLを設定する転送間隔のマルチプライヤを設定します。

<reinit-seconds> -再開までの遅延時間を設定します。

no - このコマンドによりLLDPが有効であるポートのローカルデータ送信に関する、一部またはすべてのタイミングパラメータをデフォルト値に戻します。

初期設定

Interval-seconds: 30

Hold-value: 4

Reinit-seconds: 2

コマンド・モード

9.7 システムログ管理コマンド

9.7.1 Showコマンド

9.7.1.1 show loggingコマンド

このコマンドによりログを表示します。

Syntax
show logging

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Logging Client Local Port: syslogメッセージを送信するコレクタ／リレーのポート

CLI Command Logging: CLIコマンドログのモード

Console Logging: コンソールログのモード

Console Logging Severity Filter: コンソールログへログを行う重要度の最低値。この数値以下のメッセージがログされます。

Buffered Logging: バッファされたログのモード

Syslog Logging: 設定されたsyslogホストにログを行うモード。無効に設定するとすべてのsyslogホストへのログが停止します。

Log Messages Received: ログプロセスで受信したメッセージ数。ドロップまたは無視されたメッセージも含まれます。

Log Messages Dropped: 処理できなかったメッセージ数

Log Messages Relayed: リレーされたメッセージ数

Log Messages Ignored: 無視されたメッセージ数

9.7.2 show logging buffered

このコマンドはスイッチに維持されるメッセージログを表示します。メッセージログはシステムの追跡情報を含んでいます。

Syntax
show logging buffered

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Buffered (In-Memory) Logging: メッセージログが有効であるか無効であるかを示します。

Buffered Logging Wrapping Behavior: ラッピングが有効であるか無効であるかを示します。

Buffered Log Count: ログされたメッセージ数を示します。

Message: ログされたメッセージ



メッセージログ情報は、リセットすると削除されます。

9.7.3 show logging traplog

このコマンドはスイッチに維持されるトラップログを表示します。トラップログにはラップする 256 のエントリの最大数が含まれます。

Syntax
show logging traplogs

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Number of Traps since last reset: デバイスが最後にリセットされてから発生したトラップの数

Trap Log Capacity: スイッチに保存できたトラップの最大数

Log: トラップのシーケンス番号

System Up Time: このトラップが生じたスイッチの最後の再起動以降の相対的時間

Trap: トラップの情報



トラップログ情報は、リセットすると削除されます。

9.7.3.1 show logging hosts

このコマンドによりすべての設定ログホストを表示します。

Syntax
show logging hosts

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Index

IP Address: 設定サーバのIPアドレス

Severity: 特定のアドレスにログを行う重要度の最低値

Port Server Port Number: syslogメッセージを送信したローカルホストのポート

Status ： 設定syslogホストへのログ状態。ステータスが無効の場合、ログは行われません。

9.7.4 設定コマンド

9.7.4.1 logging buffered

このコマンドにより最大 128 ログを保存できる内部メモリログへのログ実施を有効化します。

Syntax
logging buffered no logging buffered

no - このコマンドにより内部メモリログへのログ実施を無効化します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりログ可能最大数に到達した場合の内部メモリログのラッピングを有効化します。無効の場合、ログ可能最大数に到達するとログが停止します。

Syntax
logging buffered wrap no logging buffered wrap

no - このコマンドによりログ可能最大数に到達した場合の内部メモリログのラッピングを無効化します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.7.4.2 logging console

このコマンドによりコンソールへのログ実施を有効化します。

Syntax
logging console [<severitylevel> | <0-7>] no logging console

[<severitylevel> | <0-7>] -緊急 (0)、警告 (1)、重要 (2)、エラー (3)、注意 (4)、指示 (5)、通知 (6)、デバッグ (7) の内容で、0〜7 の整数で表示されます。

no - このコマンドによりコンソールへのログ実施を無効化します。

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.7.4.3 logging host

このコマンドにより最大 8 つのホストを設定できる場合にホストへのログを有効化します。

Syntax
logging host <hostaddress> [<port>] [[<severitylevel> | <0-7>]]

<hostaddress> - ログサーバのIPアドレス

<port> - ポート番号

[<severitylevel> | <0-7>] -緊急 (0)、警告 (1)、重要 (2)、エラー (3) 、注意 (4)、 指示 (5)、通知 (6)、デバッグ (7) の内容で、0〜7 の整数で表示されます。

初期設定

なし

コマンド･モード

グローバル･コンフィグ

このコマンドによりホストへのログ実施を無効化します。

Syntax
logging host remove <hostindex>

<hostindex> - ログサーバのインデックス

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりログサーバのIPアドレスを再設定します。

Syntax
logging host reconfigure <hostindex> {host <hostaddress> | port <port> | severitylevel <level>}

<hostindex> - ログサーバのIPアドレス

host -新規ログホストのIPアドレスの変更

<hostaddress> - ログサーバの新規IPアドレス

port -新規ログホストのポートの変更

<port> - <1 - 65535>の範囲の新規ポート値

severitylevel -新規ログホストの重要度の変更

[<severitylevel> | <0-7>] -緊急 (0) 、警告 (1) 、重要 (2) 、エラー (3) 、注意 (4) 、指示 (5) 、通知 (6) 、デバッグ (7) の内容で、0～7 の整数で表示されます。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.7.4.4 logging syslog

このコマンドによりsyslogのログ実施を有効化します。

Syntax
logging syslog no logging syslog

no - syslogのログ実施を無効化します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりログメッセージでのLOGクライアントのローカルポート数を設定します。

.

Syntax
logging syslog port <portid> no logging syslog port

no - ローカルログポートをデフォルト値に戻します。

<portid> - 1～65535 のポートID

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.7.4.5 clear logging buffered

このコマンドによりすべての内部メモリログをクリアします。

Syntax
clear logging buffered

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.8 スクリプト管理コマンド

9.8.1 script apply

このコマンドにより設定スクリプトのコマンドをIBPに適用します。適用コマンドにより動作設定のバックアップを行い、スクリプトファイルへのコマンド適用を開始します。コマンド適用は、コマンドが最初に失敗した時に停止します。

Syntax
script apply <scriptname>

<scriptname> -適用するスクリプト名

初期設定

なし

コマンド・モード

特権EXEC

9.8.2 script delete

このコマンドはスイッチに現れる特定のスクリプトやすべてのスクリプトを削除します。

Syntax
script delete {<scriptname> | all}

<scriptname> -削除するスクリプト名

すべて – スイッチに現れるすべてのスクリプトを削除します。

初期設定

なし

コマンド・モード

特権EXEC

9.8.3 script list

このコマンドは存在するファイルの合計数とスイッチに現れるすべてのスクリプトをリストします 。

Syntax
script list

初期設定

なし

コマンド・モード

特権EXEC



すべてのスクリプトファイルの合計サイズは 2 MBを超えることはできません。

9.8.4 script show

このコマンドによりスクリプトファイルの内容を表示します。

Syntax
script show <scriptname>

<scriptname> - スクリプトファイル名

初期設定

なし

コマンド・モード

特権EXEC

9.9 システムユーティリティ

9.9.1 clear

9.9.1.1 clear arp

このコマンドにより動的タイプのすべてのARPエントリを、ARPキャッシュから削除します。

Syntax
clear arp

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.2 clear traplog

このコマンドによりトラップログをクリアします。

Syntax
clear traplog

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.3 clear eventlog

このコマンドによりシステムからのエラーメッセージが含まれたイベントログをクリアします。

Syntax
clear eventlog

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.4 clear logging buffered

このコマンドはスイッチに維持されるメッセージログをクリアするために使われます。メッセージログにはシステムログ情報が含まれています 。

Syntax
clear logging buffered

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.5 clear config

このコマンドはスイッチの電源を切らずに構成を工場デフォルトへリセットします。このスイッチはこのコマンドが実行されると自動的にリセットされます。リセット実施前に確認メッセージが表示されます。

Syntax
clear config

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.6 clear pass

このコマンドはすべてのユーザーのパスワードをスイッチの電源を切らずに工場デフォルトへリセットします。パスワードのリセット実施前に確認メッセージが表示されます。

Syntax
clear pass

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.7 clear counters

このコマンドは特定の<slot/port>の統計または引数に基づいてすべてのポートやスイッチ全体の統計をクリアします。

Syntax
clear counters [<slot/port> | all]

<slot/port> -必要なインターフェイス番号である

all - すべてのインターフェイス。

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.8 clear dns counter

このコマンドでDNS統計データをクリアします。

Syntax
clear dns counter

初期設定

なし

コマンド･モード

特権EXEC

9.9.1.9 clear dns cache

このコマンドによりDNSキャッシュからすべてのエントリをクリアします。

Syntax
clear dns cache

初期設定

なし

コマンド･モード

特権EXEC

9.9.1.10 clear cdp

このコマンドはCDP周辺情報とCDPパケットカウンターをクリアするために使われます。

Syntax
clear cdp [traffic]

traffic – このコマンドはCDPパケットカウンターをクリアするために使われます。

デフォルトセッティング

なし

コマンドモード

特権EXEC

9.9.1.11 clear vlan

このコマンドはVLAN構成パラメータを工場デフォルトへリセットします。

Syntax
clear vlan

デフォルトセッティング

なし

コマンドモード

特権EXEC

9.9.1.12 enable passwd

このコマンドにより特権EXECのパスワードを変更します。

Syntax
enable passwd {0 | 7} <password>

0 - プレーンテキストのパスワードを示します。

7 - 暗号化形式のパスワードを示します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.9.1.13 clear igmp snooping

このコマンドによりIGMPスヌーピング機能で管理されているテーブルをクリアし、マルチキャスト転送データベースからそのエントリの削除を試行します。

Syntax
clear igmp snooping

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.14 clear mld snooping

このコマンドによりMLDスヌーピング機能で管理されているテーブルをクリアし、マルチキャスト転送データベースからそのエントリの削除を試行します。

Syntax
clear mld snooping

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.15 clear port-channel

このコマンドによりすべてのポートチャネル (LAG) をクリアします。

Syntax
clear port-channel

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.16 clear port-security dynamic

このコマンドによりすべてのポートセキュリティ動的情報をクリアします。

Syntax
clear port-security dynamic {address <mac-addr> | interface <slot/port>}

address - MACアドレスの動的アドレスをクリアします。

<mac-addr> - MACアドレス

interface - インターフェイスの動的アドレスをクリアします。

<slot/port> -必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.17 clear ip filter

このコマンドによりすべてのipフィルターエントリをクリアします。

Syntax
clear ip filter

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.18 clear ipv6 statistics

このコマンドによりIPv6 統計データをリセットします。

Syntax
clear ipv6 statistics {oob | switchport}

oob - アウトバウンドのIPv6 統計データをクリアします。

switchport - インバウンドのIPv6 統計データをクリアします。

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.19 clear dot1x statistics

このコマンドにより特定のポートまたはすべてのポートの 802.1x統計データをリセットします。

Syntax
clear dot1x statistics {all | <slot/port>}

<slot/port> - 必要なインターフェイス番号である。

all - すべてのインターフェイス。

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.20 clear radius statistics

このコマンドによりすべてのRADIUS統計データをクリアします。

Syntax
clear radius statistics

初期設定

なし

コマンド･モード

特権EXEC

9.9.1.21 clear tacacs

このコマンドによりTACACS+設定をクリアします。

Syntax
clear tacacs

初期設定

なし

コマンド･モード

特権EXEC

9.9.1.22 clear lldp

このコマンドによりLLDP統計データをクリアします。

Syntax
clear lldp {remote-data | statistics}

remote-data - lldpリモートデータをクリアします。

statistics - lldp統計データをクリアします。

初期設定

なし

コマンド・モード

特権EXEC

9.9.1.23 clear vtp statistics

このコマンドはVTP構成をデフォルトへリセットするために使われます。

Syntax
clear vtp statistics

デフォルト設定

なし

コマンドモード
特権EXEC

9.9.2 copy

このコマンドはスイッチへアップロード･スイッチからダウンロードします。ローカルのURLはtftpやxmodemにより特定されます。次のものがスイッチからアップロードするソースファイルとして特定されます:IBPからアップロードを行うソースファイルに、開始設定 (startup-config) 、イベントログ (eventlog) 、メッセージログ (msglog) 、トラップログ (traplog) を指定できます。宛先はURLで指定されます。

このコマンドによりURLにソース、および開始設定またはイメージに宛先を指定し、開始設定またはコードイメージをダウンロードできます。

このコマンドにより動作設定にソース、および開始設定{*filename*}に宛先を指定し、動作設定をフラッシュメモリに保存できます。

また、このコマンドによりsshkey-rsa、sshkey-rsa2、sshkey-dsaのsshキーファイル、またsslpem-root、sslpem-server、sslpem-dhweak、sslpem-dhstrongのhttpセキュアサー バ証明書をダウンロ ードできます。

9.9.2.1 copy upload File

Syntax

```
copy startup-config <sourcefilename> <url>
copy {errorlog | log | traplog} <url>
copy script <sourcefilename> <url>
copy image <filename> <url>

where <url>={xmodem | tftp://ipaddr/path/file | ftp://user:pass@ipaddr/path/file}
```

<sourcefilename> -設定ファイルまたはスクリプトファイルのファイル名
<url> - xmodem or tftp://ipaddr/path/file or ftp://user:pass@ipaddr/path/file.
errorlog - イベントのログファイル
log - メッセージのログファイル
traplog - トラップのログファイル
<filename> -設定ファイル名またはイメージファイル名

初期設定
なし
コマンド･モード
特権EXEC

9.9.2.2 **copy download File**

Syntax
copy <url> startup-config <destfilename> copy <url> image <destfilename> copy <url> {sshkey-rsa1 | sshkey-rsa2 | sshkey-dsa} copy <url> {sslpem-root | sslpem-server | sslpem-dhweak | sslpem-dhstrong} copy <url> script <destfilename> where <url>={xmodem | tftp://ipaddr/path/file | ftp://user:pass@ipaddr/path/file}

<destfilename> - イメージファイル名またはスクリプトファイル名

<url> - xmodem or tftp://ipaddr/path/file or ftp://user:pass@ipaddr/path/file.

sshkey-rsa1 - SSH RSA1 キーファイル

sshkey-rsa2 - SSH RSA2 キーファイル

sshkey-dsa - SSH DSAキーファイル

sslpem-root - Secure Root PEMファイル

sslpem-server - Secure Server PEMファイル

sslpem-dhweak - Secure DH Weak PEMファイル

sslpem-dhstrong - Secure DH Strong PEMファイル

初期設定

なし

コマンド･モード

特権EXEC

9.9.2.3 copy running-config startup-config

Syntax
copy running-config startup-config [filename]

<filename> -設定ファイル名

初期設定

なし

コマンド・モード

特権EXEC

9.9.2.4 copy clibanner

Syntax
copy clibanner <url> copy <url> clibanner no clibanner

<url> - tftp://ipaddr/path/file or ftp://user:pass@ipaddr/path/file.

no - CLIバナーを削除します。

初期設定

なし

コマンド・モード

特権EXEC

9.9.2.5 copy file running-config

Syntax
copy file running-config

初期設定

なし

コマンド・モード

特権EXEC

9.9.3 delete

このコマンドにより設定ファイルまたはイメージファイルを削除します。

Syntax
delete <filename>

<filename> -設定ファイル名またはイメージファイル名

初期設定

なし

コマンド・モード

特権EXEC

9.9.4 dir

このコマンドによりフラッシュメモリ上のファイルのリストを表示します。

Syntax
dir [boot-rom	config	opcode [<filename>]]

<filename> - 必要なインターフェイス番号である。

boot-rom - bootrom.

config -設定ファイル

opcode - ランタイム動作コード

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

列見出し	説明
date	ファイル作成日
file name	ファイル名
file type	ファイルタイプ：ブートROM、動作コード、設定ファイル
startup	システム開始時にこのファイルを使用するかを示します。
size	バイト単位のファイルの長さ

9.9.5 whichboot

このコマンドによりシステム開始時にブートしたファイルを表示します。

Syntax
whichboot

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Boot-System: 現在のブートモード

Next Booting Mode: リブート後のブートモード

file name: 必要なインターフェイス番号である。

file type: ブートROMイメージ、動作コード、または設定ファイル

startup: ブート時に使用します。

size (byte): 設定ファイルまたはイメージファイルのサイズ

9.9.6 boot-system

このコマンドによりシステム開始に使用するファイルまたはイメージを指定します。

Syntax
boot-system {boot-rom | config | opcode | auto-copy-sw} <filename> boot-system mode {switch | IBP}

<filename> - **必要なインターフェイス番号である。**

boot-rom - bootrom.

config - **設定ファイル**

opcode - **ランタイム動作コード**

mode - SwitchまたはIBPに切り替えます。

(*)auto-copy-sw - **スタックシステムの自動アップグレード機能を設定します。**

注記: (*)はスタッキングコマンドです。

初期設定

なし

コマンド・モード

特権EXEC

9.9.7 ping

このコマンドにより別のコンピュータがネットワーク上にあり、接続に応答するかを確認します。このコマンドを使うためには、ネットワーク(インバンド)接続のためにスイッチを構成します。ソースとターゲットのデバイスはPing･ユーティリティーを有効化しTCP/IPの一番上で稼働している必要があります。スイッチはスイッチがデフォルトVLAN(VLAN1)を通じて接続されている任意のIPワークステーションから、スイッチとワークステーションの間に物理パスが通っている限りPingできます。終端のインターフェイスはターゲットステーションへ 3 つPingを送ります 。

Syntax
ping <host>

<host> - ホスト名またはIPアドレス

初期設定

なし

コマンド･モード

特権EXEC

9.9.7.1 ping <host> count [size]

Syntax
ping <host> count <0-20000000> [size <32-512>] ping <host> size <32-512> [count <0-20000000>]

<host> - ホスト名またはIPアドレス

<0-20000000> - pingの数 (範囲：0～20000000) 。注記：0 は無限を示します。

<size> - パケットサイズ (範囲：32～512)

初期設定

Count = 5

Size = 32

コマンド･モード

特権EXEC

9.9.7.2 **ping ipv6**

Syntax
ping ipv6 <ipv6-address>

<ipv6-address> - IPv6 アドレス

初期設定

なし

コマンド・モード

特権EXEC

9.9.7.3 **ping ipv6 interface**

Syntax
ping ipv6 interface {oob | switchport} <link-local-address> [size <datagram-size>]

oob - out-of-bandのインターフェイス

switchport -インバンドのインターフェイス

<link-local-address> - リンクローカルアドレス

<datagram-size> - データグラムサイズ (範囲:48～2048)

初期設定

なし

コマンド・モード

特権EXEC

9.9.8 traceroute

このコマンドによりパケットがホップごとにネットワーク経由で宛先に送信された際に、実際に通過するルートを確認します。<ipaddr>は有効なIPである必要があります。[port]は 0～65535 の範囲の有効な 10 進法の整数である必要があります。デフォルト値は 33434 です。任意のポートパラメータは、トレースルートの一部として送信されたパケットの宛先に使用される、UDPポートです。このポートは、宛先のシステム上の未使用ポートである必要があります。

Syntax
traceroute <ipaddr|hostname> [initTtl <1-255>] [maxTtl <1-255>] [interval <1-60>] [count <1-10>] traceroute ipv6 <ipv6-address> [initTtl <1-255>] [maxTtl <1-255>] [interval <1-60>] [count <1-10>]

<ipaddr|hostname> - ホスト名またはIPアドレス

initTtl - 使用する初期TTL

<1-255> - 範囲：1～255

maxTtl - 宛先の最大TTL

<1-255> - 範囲：1～255

Interval - プローブの秒単位の間隔

<1-60> - 範囲：1～60

count - 1 ホップあたりのプローブ数

<1-10> - 範囲：1～10

<ipv6-address> - IPv6 アドレス

初期設定

initTtl = 1

maxTtl = 20

interval = 3

count = 3

コマンド・モード

特権EXEC

9.9.9 logging cli-command

このコマンドはCLIコマンド･ロギング機能を有効化します。コマンドロギングコンポーネントはスイッチがシステムで発行されるすべてのコマンドラインインターフェイス(CLI)コマンドを記録することを可能にします。

Syntax
logging cli-command

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.9.10 calendar set

このコマンドによりシステム時計を設定します。

Syntax
calendar set <mm/dd/yyyy> <hh:mm:ss>

<mm/dd/yyyy> - 月 (範囲：1～12) 、日 (範囲：1～31) 、年 (4 桁。範囲：2000～2099)

<hh:mm:ss> - 24 時間形式、hh (時間。範囲：0～23) 、mm (分。範囲：0～59) ss (秒。範囲：0～59)

初期設定

なし

コマンド･モード

特権EXEC

9.9.11 reload

このコマンドは電源を切らずにスイッチをリセットします。リセットとはすべてのネットワーク接続が終了され、ブートコードが実行されることを意味します。スイッチは保存された構成によりスイッチを初期化します。リセットを続けるべきかどうかの確認を促されます。リセットに成功すればその旨がスイッチのLEDで表示されます。

Syntax
reload [slot <unit>]

(*)slot – スタックまたはスタックのスイッチをリロードします。

(*)<unit> - 1～8 のスイッチIDまたはCB名

注記：(*) はスタッキングコマンドです。

初期設定

なし

コマンド・モード

特権EXEC

9.9.12 Configure

このコマンドによりグローバル設定モードをアクティブ化します。

Syntax
configure

初期設定

なし

コマンド・モード

特権EXEC

9.9.13 disconnect

このコマンドによりtelnetセッションを閉じます。

Syntax
disconnect {<0-42> | all}

<0-42> - リモートセッションID

all - すべてのリモートセッション

初期設定

なし

コマンド・モード

特権EXEC

9.9.14 hostname

このコマンドによりプロンプト文字列を設定します。

Syntax
hostname <prompt_string>

< prompt_string > - プロンプト文字列

初期設定

CB

コマンド・モード

グローバル・コンフィグ

9.9.15 pager

このコマンドによりページャー設定を有効化／無効化します。

Syntax
pager no pager

no - このコマンドによりページャー機能を無効化します。

初期設定

なし

コマンド・モード

特権EXEC

9.9.16 do

このコマンドによりグローバル設定モードまたは設定サブモードから特権 EXEC-levelコマンドを実行します。

Syntax
do [EXEC-level command]

[EXEC-level command] - 特権 EXEC Commandモードの特権EXEC-levelコマンド

初期設定

なし

コマンド・モード

グローバル・コンフィグ、設定サブモード

9.9.17 quit

このコマンドによりCLIセッションを終了します。

Syntax
quit

初期設定

なし

コマンド・モード

特権EXEC

9.10 スパニングツリー・コマンド

この節はスパニングツリー・コマンドの詳しい説明を提供します。IEEE要件に準拠するため、基本的なスパニングツリー(STP 802.1d)は削除され、そのSTPはマルチスパニングツリー(MSTP 802.1s)の段階でシミュレートされます。従って、基本の 5 つの段階は旧来のフェイズとは違っています。それは基本のスパニングツリー機能に影響を与えません。これはコンフリクトの観点ではありません。

コマンドは 2 つの機能グループに分けられます:

- 表示コマンドはスパニングツリーの設定、統計、ほかの情報を表示します。
- 構成コマンドはスイッチの機能とオプションを構成します。各構成コマンドに対して、構成セッティングを表示する表示コマンドがあります。

9.10.1 Show コマンド

9.10.1.1 show spanning-tree

このコマンドは共通する内部のスパニングツリーのスパニングツリー設定を表示します。以下の詳細が表示されます。

Syntax
show spanning-tree

デフォルト設定

なし

コマンドモード

特権EXEC

メッセージを表示

Bridge Priority: 値を構成します.

Bridge Identifier: ブリッジ識別子がスパニングツリー・アルゴリズムとプロトコルに使用されるブリッジのMACアドレス

Time Since Topology Change: 経過時間 。

Topology Change Count: 変更回数。

Topology Change in progress: トポロジーの変更が共通する内部スパニングツリーに割当てられた任意のポートで進行中かどうかを示すスイッチのトポロジー変更値 。

Designated Root: MSTIDに識別されたスパニングツリー・インスタンスのルートブリッジのブリッジ識別子。

Root Path Cost: 共通な内部スパニングツリーのためのルートパス・コスト・パラメータ値

Root Port Identifier: MSTIDに識別されたスパニングツリーのインスタンスのルートポート

Bridge Max Age: 最大メッセージエイジ

Bridge Max Hops: スパニングツリーのためのホップの最大数

Bridge Forwarding Delay: ブリッジされたLANのすべてのブリッジに使用されるタイムアウト値。転送の遅延はルートにより設定されます。

Hello Time: 構成BPDUの生成の間隔

Bridge Hold Time: 構成ブリッジプロトコルデータユニット(BPDU)の送信の最小時間

CST Regional Root: 現在のCST局所ルートのブリッジ識別子

Regional Root Path Cost: 局所ルートへのパス･コスト値

Associated FIDs: このインスタンスに現在関連付けられた転送データベースの識別子のリスト。

Associated VLANs: このインスタンスに現在関連付けられたVLAN IDのリスト。

9.10.1.2 show spanning-tree interface

このコマンドは共通する内部のスパニングツリー内の特定のスイッチポート設定とパラメータを表示します。<slot/port>は希望するスイッチポートです。次の詳細はコマンドの実行時に表示されます。

Syntax
show spanning-tree interface <slot/port>

希望するインターフェイス番号です。

デフォルト設定

なし

コマンドモード

特権EXEC

メッセージを表示

Port Mode: スパニングツリーの管理モード

Port Up Time Since Counters Last Cleared: ポートがリセットされて以降の時間、日、時間、分、秒数で表示します。

BPDUFilter: 現在ポート(STPモード)でのBPDUフィルターのステータス

BPDUGuard: 現在ポート(STPモード)でのBPDUガードモード。

Loop Guard: 現在ポート(STPモード)でのループガードモード。
ルートガード: 現在ポート(STPモード)でのルートガードモード.、
Root Guard: 送信されたスパニングツリープロトコルブリッジプロトコル･データユニット。

STP BPDUs Received: 送信されたスパニングツリープロトコルブリッジプロトコル･データユニット。

RST BPDUs Transmitted: 送信された高速スパニングツリープロトコルブリッジプロトコルデータユニット。

RST BPDUs Received: 受信した高速スパニングツリープロトコルブリッジプロトコルデータユニット。

MSTP BPDUs Transmitted: マルチプル･スパニングツリープロトコルブリッジプロトコルデータユニット。
MSTP BPDUs Received: マルチプル･スパニングツリープロトコルブリッジプロトコルデータユニット。

9.10.1.3 show spanning-tree vlan

このコマンドはVLANとマルチプルスパニングツリーのインスタンスとの関連を表示します。<1-4094>が既存VLAN IDに対応します 。

Syntax
show spanning-tree vlan <1-4094>

<vlanid> - VLAN ID(範囲 1～4094)

初期設定

なし

コマンドモード

特権EXEC

メッセージを表示

VLAN Identifier: VLAN IDを表示します。

Associated Instance: 関連付けられたマルチプル･スパニングツリーインスタンスまたは、共通する内部のスパニングツリーに関連付けられた場合の｢CST｣のための識別子。

9.10.1.4 show spanning-tree mst

このコマンドは特定のマルチプル･スパニングツリーのインスタンスの設定とパラメータを表示します。<0-4094>のインスタンスは希望する既存マルチプル･スパニングツリーインスタンスに対応する番号です。

Syntax
show spanning-tree mst detailed <0-4094>

<0-4094> - マルチプル･スパニングツリーインスタンスID

初期設定

なし

コマンドモード

特権EXEC

メッセージを表示

MST Instance ID: マルチプルスパニングツリーインスタンスID

MST Bridge Priority: 現在MSTのブリッジプライオリティ

MST Bridge Identifier: 現在MSTのブリッジID

Time Since Topology Change: 経過時間 。

Topology Change Count: このマルチプルスパニングツリーインスタンスに対してトポロジーが変更された回数

Topology Change in Progress: マルチプルスパニングツリーインスタンスへのトポロジー変更パラメータの値。

Designated Root: マルチプルスパニングツリーインスタンスへの局所ルートの識別子。

Root Path Cost: このマルチプルスパニングツリーインスタンスのための指定されたルートへのパス·コスト。

Root Port Identifier: このマルチプルスパニングツリー·インスタンスのための指定されたルートへアクセスするポート。

Associated FIDs: このインスタンスに関連付けられたデータベースを転送jする識別子のリスト。

Associated VLANsこのインスタンスに関連付けられたVLAN IDのリスト。

このコマンドはスイッチのすべてのマルチプルスパニングツリーインスタンスについての概要情報を表示します。実行すれば、次の詳細が表示されます。

Syntax
show spanning-tree mst summary

初期設定

なし

コマンドモード

特権EXEC

メッセージを表示

MST Instance ID List: 現在構成されているマルチプルスパニングツリーIDのリスト。

For each MSTID: マルチプルスパニングツリーインスタンスID。

Associated FIDs: このインスタンスに関連付けられたデータベースを転送識別子のリスト。

Associated VLANs: このインスタンスに関連付けられたVLAN IDのリスト。

このコマンドは特定のマルチプルスパニングツリーインスタンスにおける特定のスイッチポートのための詳しい設定とパラメータを表示します。<msid>インスタンスは希望する既存マルチプルスパニングツリーインスタンスへ対応する番号です。<slot/port>は希望するスイッチポートです。

Syntax
show spanning-tree mst port detailed <0-4094> <slot/port>

<0-4094> - マルチプルスパニングツリーインスタンスID。

<slot/port> - これは希望するインターフェイス番号です。

初期設定

なし

コマンドモード

特権EXEC

メッセージを表示

MST Instance ID: マルチプルスパニングツリーインスタンスID

Port Identifier: そのブリッジのポートを識別する固有値です。

Port Priority: MST内のポートのプライオリティ。

Port Forwarding State: このポートの現在のスパニングツリー状態です。

Port Role: ポートの役割がルートか指定かを示します。

Auto-calculate Port Path Cost: ポートの自動計算によるポートパス･コストを表示します。

Port Path Cost: 内部のポートパス･コスト変数の構成された値。

Designated Root: このポートの指定されたルートの識別子。

Designated Port Cost: 指定されたポートからLANに提供されたパス･コスト。

Designated Bridge: 指定されたポートがあるブリッジを指すブリッジ識別子

Designated Port Identifier: LANへの最小のコストを提供する指定されたブリッジ上のポート

0 (デフォルトCIST IDに定義)が<0-4094>として通ればこのコマンドは共通する内部スパニングツリー内の特定のスイッチポートのための設定とパラメータを表示します。<slot/port>は希望するスイッチポートです。この場合、次の情報が表示されます。

Port Identifier: CST内のこのポートのためのポート識別子

Port Priority: CST内のポートのプライオリティ。

Port Forwarding State: CST内のポートの転送状態。

Port Role: CST内の特定のインターフェイスの役割。

Auto-calculate Port Path Cost: ポートの自動計算によるポートパス･コストを表示します。

Auto-calculate External Port Path Cost – 外部パス･コストを自動で計算する(有効)かしないか(無効)を表示します。外部のパス･コスト値は外部ポートパス･コストがゼロに構成されている場合ポートのリンク速度に基づいてパス･コストが計算されます。

External Port Path Cost: スパニングツリーにある特定のポートの外部パス･コスト。

Port Path Cost: 特定のインターフェイスのための構成されたパス･コスト。

Designated Root: CST内のこのポートのための指定されたルートの識別子。

Designated Port Cost: 指定されたポートがLANに提供するパス・コスト。

Designated Bridge: 指定されたポートを含むブリッジ。

Designated Port Identifier: LANへ最小のコストを提供する指定されたブリッジのポート。

Topology Change Acknowledgement: このポートのためにトポロジーの変更が進行中かどうかを示す次の構成ブリッジプロトコルデータユニット(BPDU)送信におけるフラッグの値。

Hello Time: このポートに使用中のhelloタイム。

Edge Port: このポートがエッジポートかどうかを示す構成された値。

Edge Port Status: エッジポートステータス。エッジポートとして動作している場合「真」、そうでなければ「偽」を示します 。

Point To Point MAC Status: このポートが点間リンクの一部かどうかを示す 。

CST Regional Root: このポートに使用される局所ルート識別子。

CST Port Cost: このポートのための構成パス・コスト。

このコマンドは特定のマルチプルスパニングツリーインスタンス内の1個またはすべてのポートの設定を表示します。<0-4094>のパラメータは特定のMSTインスタンスを示します。{<slot/port> | all}のパラメータは希望のスイッチポートかすべてのポートを示します。

0 (デフォルトCIST IDに定義)が<0-4094>として通れば、そうすればステータス概要が1個またはすべての共通する内部スパニングツリー内にあるポートについて表示されれます。

Syntax
show spanning-tree mst port summary <0-4094> {<slot/port> | all}

<0-4094> - マルチプルスパニングツリーインスタンス ID

<slot/port> -必要なインターフェイス番号です。

すべて - すべてのインターフェイス。

初期設定

なし

コマンドモード

特権EXEC

メッセージを表示

MST Instance ID: このポートに関連付けられたMSTインスタンス。

Interface: インターフェイス表示される予定です。

STP Mode: STPモードを示します。

Type: 現在使用されていない。

STP State: 特定のスパニングツリーインスタンスにあるポートの転送状態。

Port Role:スパニングツリー内の特定のポートの役割。

9.10.1.5 show spanning-tree summary

このコマンドはスイッチのスパニングツリーの設定とパラメータを表示します。次の詳細がコマンドの実行で表示されます。

Syntax
show spanning-tree summary

初期設定

なし

コマンドモード

特権EXEC

メッセージを表示

Spanning Tree Adminmode: 有効化または無効化。

Spanning Tree Forward BPDU: 有効化または無効化。

Spanning Tree Version: フォース･プロトコルのバージョンパラメータに基づいて現在サポートされている (IEEE 802.1s, IEEE802.1w、または IEEE802.1d)802.1 のバージョン。

Configuration Name: T構成された名前。

Configuration Revision Level: 構成値。

Configuration Digest Key: 計算値。

Configuration Format Selector: 構成値。.

MST Instances: スイッチ上で構成されたすべてのマルチプルスパニングツリーインスタンスのリスト。

9.10.1.6 show spanning-tree brief

このコマンドはブリッジのためのスパニングツリー設定を表示します。 この場合、次の詳細が表示されます。

Syntax
show spanning-tree brief

初期設定

なし

コマンドモード

特権EXEC

メッセージを表示

Bridge Priority: 設定された値 .

Bridge Identifier: 現在スパニングツリーのブリッジID。

Bridge Max Age: 構成値。

Bridge Max Hops: 値を構成します

Bridge Hello Time: 値を構成します

Bridge Forward Delay: 値を構成します

Bridge Hold Time: ブリッジプロトコルデータユニット(BPDU)構成の送信間の最小時間。

9.10.2 Configコマンド

9.10.2.1 spanning-tree

このコマンドはスパニングツリーモードを有効化します。

Syntax
spanning-tree no spanning-tree

no - このコマンドはスパニングツリーモードを無効化します。無効化されると、スパニングツリー構成は保持され変更できますが、アクティブにはできません。

初期設定

無効

コマンドモード

グローバル・コンフィグ

9.10.2.2 spanning-tree protocol-migration

このコマンドはインターフェイスでのBPDUの移動チェックを有効化します。「すべての(all)」オプションはすべてのインターフェイスでのBPDUの移動チェックを有効化します。

Syntax
spanning-tree protocol-migration {<slot/port> | all}

<slot/port> - は希望するインターフェイス番号です。

all – すべてのインターフェイス

初期設定

なし

コマンドモード

グローバル・コンフィグ

9.10.2.3 **spanning-tree configuration**

このコマンドはスイッチが現在使っている構成を識別するために使用する構成識別名を設定します。<name>は最大 32 の英数字の文字列です。

Syntax
spanning-tree configuration name <name> no spanning-tree configuration name

<name> -最大 32 文字の英数字の文字列です。

no - このコマンドは構成識別子名をデフォルトへリセットします。

初期設定

IEEE 802 基準に特定された 16 進法の表記法により表示されたベースのMACアドレス。

コマンドモード

グローバル･コンフィグ

このコマンドはスイッチが現在使っている構成を識別するために使用する構成リビジョンレベルを設定します。構成改訂レベルは 0 から 65535 の範囲の数字です 。

Syntax
spanning-tree configuration revision <0-65535> no spanning-tree configuration revision

<value> -改訂レベルは 0 から 65535 の範囲の数字です。

no -このコマンドはスイッチが現在使っている構成を識別するために使用する構成リビジョンレベルをデフォルト値の 0 へ設定します 。

初期設定

0

コマンドモード

グローバル･コンフィグ

9.10.2.4 spanning-tree mode

このコマンドは強制プロトコルバージョンパラメータを新しい値に設定します。強制プロトコルバージョンは次のうちのどれかです。

1. stp – ST BPDU が MST BPDU(IEEE802,1d 機能性がサポートされている)が送信されます 。
2. rstp – RST BPDU(IEEE 802,1w の機能性がサポートされている)が送信されます 。
3. mstp – MST BPDU が送信されます。(IEEE 802.1s の機能性がサポートされている)

Syntax
spanning-tree mode {stp | rstp | mstp}

初期設定

mstp

コマンドモード

グローバル･コンフィグ

9.10.2.5 spanning-tree bpdu forwarding

このコマンドはBPDU転送機能を有効化または無効化します。BPDUの転送機能はBPDUパケットの転送を許可または拒否するように設定できます。

Syntax
spanning-tree bpdu-forwarding no spanning-tree bpdu-forwarding

no - このコマンドはBPDU転送モードのパラメータをデフォルト、すなわち有効化します。

初期設定

有効

コマンドモード

グローバル･コンフィグ

9.10.2.6 spanning-tree edgeport

このコマンドはエッジポート機能をスイッチに有効化または無効化します。

Syntax
spanning-tree edgeport no spanning-tree edgeport

no - このコマンドはエッジポート機能をデフォルトに設定、すわなち有効化します。

初期設定

有効

コマンドモード

グローバル・コンフィグ

このコマンドはエッジポート機能をこのインターフェイス上で有効化または無効化します。

Syntax
spanning-tree edgeport no spanning-tree edgeport

no - このコマンドはエッジポートの機能をデフォルトに設定、すなわち有効化します。

初期設定

有効

コマンドモード

インターフェイスの構成

このコマンドはスイッチ上のBPDUの送受信のためのエッジポートBPDUフィルターの/無効パラメータを設定します。 このコマンドはdot1dモードでのみす。

Syntax
spanning-tree edgeport bpdufilter no spanning-tree edgeport bpdufilter

no - このコマンドはエッジポートBPDUフィルターをデフォルトに設定、すなわち無効化します。

初期設定

無効

コマンドモード

グローバル・コンフィグ

このコマンドはスイッチでBPDUを処理するエッジポートBPDUガードの有効化/無効化パラメータを設定します 。

Syntax
spanning-tree edgeport bpduguard no spanning-tree edgeport bpduguard

no - このコマンドはエッジポートのBPDUガードをデフォルトに設定、すなわち無効化します。

初期設定

無効

コマンドモード

グローバル・コンフィグ

このコマンドはインターフェイス上のBPDUを送受信するエッジポートBPDUフィルターの有効化/無効化パラメータを設定します。

Syntax
spanning-tree bpdufilter no spanning-tree bpdufilter

no - このコマンドはエッジポートのフィルターをデフォルト値に設定、すなわち無効化します。

初期設定

無効

コマンドモード

インターフェイス・コンフィグ

このコマンドはインターフェイスでBPDUを処理するエッジポートBPDUガードの有効化/無効化パラメータを設定します。このコマンドはdot1dモードでのみす 。

Syntax
spanning-tree edgeport bpduguard no spanning-tree edgeport bpduguard

no - このコマンドはエッジポートBPDUガードをデフォルト値に設定、すなわち無効化します。

初期設定

無効

コマンドモード

インターフェイス・コンフィグ

9.10.2.7 spanning-tree uplinkfast

このコマンドはアップリンク･ファーストのパラメータをこのスイッチ上で新しい値に設定します。このコマンドはdot1dモードでのみ機能します。

Syntax
spanning-tree uplinkfast no spanning-tree uplinkfast

no - このコマンドはアップリンク･ファーストのパラメータをデフォルト値に設定、すなわち無効化します。

初期設定

無効

コマンド･モード

グローバル･コンフィグ

9.10.2.8 spanning-tree loopguard

このコマンドはこのスイッチ上のループガードのパラメータを新しい値に設定します。このコマンドはdot1dモードでのみ機能します。

Syntax
spanning-tree loopguard no spanning-tree loopguard

no - このコマンドは強制プロトコルバージョンのパラメータをデフォルトに設定、すなわち無効化します。

初期設定

無効

コマンド･モード

グローバル･コンフィグ

このコマンドは強制プロトコルバージョンのパラメータをこのインターフェイス上で新しい値に設定します。このコマンドはdot1dモードでしか動作しません。

Syntax
spanning-tree loopguard no spanning-tree loopguard

no - このコマンドは強制プロトコルバージョンのパラメータをデフォルト値に設定、すなわち無効化します。.

初期設定

無効

コマンド・モード

インターフェイス・コンフィグ

このコマンドはガードモードのパラメータをインターフェイス上で新しい値に設定します。
このコマンドはdot1dモードでしか動作しません。

Syntax
spanning-tree guard {loop|none|root} no spanning-tree guard

loop – このコマンドはガードモードをこのインターフェイス上でループガードに設定します 。

none – このコマンドはガードモード無効に設定します 。

root – このコマンドはガードモードをこのインターフェイス上でルートガードに設定します 。

no - このコマンドはガードモードをデフォルトすなわち無効に設定します 。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

9.10.2.9 spanning-tree forward-time

このコマンドはブリッジ転送遅延のパラメータを共通する内部のスパニングツリーに対して新しい値に設定します。転送時間値は 4～30 の秒数で、その値は「ブリッジ最大エイジ/2」 + 1 」に等しいかそれより大きいです。

Syntax
spanning-tree forward-time <4-30> no spanning-tree forward-time

<4-30> -転送時間値(範囲 4～30)

no - このコマンドは共通する内部のスパニングツリーのためのブリッジ転送遅延パラメータをデフォルト値に設定、すなわち 15 に設定します。

初期設定

15

コマンド・モード

グローバル・コンフィグ

9.10.2.10 spanning-tree hello-time

このコマンドは共通する内部スパニングツリーのためのhelloタイムパラメータを新しい値に設定します。helloタイム値は「ブリッジ最大エイジ/2」 - 1 」に等しいかそれより小さい 1 から 10 までの範囲の秒数です。

Syntax
spanning-tree hello-time <1-10> no spanning-tree hello-time

<1-10> - helloタイム値(範囲 1～10)

no - このコマンドは共通する内部のスパニングツリーに対するhelloタイムのパラメータをデフォルトすなわち 2 に設定します。

初期設定

2

コマンド・モード

グローバル・コンフィグ

9.10.2.11 spanning-tree max-age

このコマンドは共通する内部スパニングツリーについてのブリッジ最大エイジパラメータを新しい値に設定します。最大エイジ値は 6 から 40 の秒数で､｢(ブリッジ転送遅延 －1)の 2 倍｣と同じかそれ以下で､かつ､｢(ブリッジhelloタイム + 1)の 2 倍｣と同じかそれより大きい値でなければならない。

Syntax
spanning-tree max-age <6-40> no spanning-tree max-age

<6-40> - ブリッジ最大エイジの値(範囲 6～40)

no - このコマンドは共通する内部のスパニングツリーのためのブリッジ最大エイジパラメータをデフォルトすなわち 20 に設定します。

初期設定

20

コマンド･モード

グローバル･コンフィグ

9.10.2.12 spanning-tree max-hops

このコマンドは共通する内部スパニングツリーのためにMSTP最大ホップのパラメータを新しい値に設定します｡最大ホップの値は 1 から 127 までの間です。

Syntax
spanning-tree max-hops <1-127> no spanning-tree max-hops

<1-127> - 最大ホップの値(範囲 1～127)

no - このコマンドは共通する内部スパニングツリーのブリッジ最大ホップパラメータをデフォルト値に設定します。

初期設定

20

コマンド･モード

グローバル･コンフィグ

9.10.2.13 spanning-tree mst

このコマンドはマルチプルスパニングツリー･インスタンスをスイッチに追加します。<1-4094>のインスタンスは追加される新しいインスタンスIDに対応する 1 から 4094 の範囲でなければなりません。サポートされるマルチプルインスタンスの最大数は 4 です。

Syntax
spanning-tree mst instance <1-4094> no spanning-tree mst instance <1-4094>

<1-4094> - マルチプルスパニングツリーインスタンスID

no - このコマンドはマルチプルスパニングツリーインスタンスをスイッチから削除して、削除されたインスタンスに割当てられていたすべてのVLANを共通する内部のスパニングツリーへ再割当てします。

初期設定

なし

コマンド･モード

グローバル･コンフィグ

このコマンドは特定のマルチプルスパニングツリー･インスタンスのためのブリッジプライオリティを設定します。インスタンス<mstid>は希望する既存マルチプルスパニングツリー･インスタンスに対応する番号です。このプライオリティの値は 4096 に 1 でインクリメントする 0 から 61440 の範囲の数字でなければなりません。

0(デフォルトのCIST IDに定義されたもの)が<mstid>で合致した場合、このコマンドは共通する内部スパニングツリーにブリッジプライオリティのパラメータを新しい値に設定します。ブリッジプライオリティの値は 0 から 61440 の範囲の数字でなければなりません。12 の重要度の最低なビットは 802.1s規格に従ってマスクされます．このプライオリティは端数の切り下げにより次に低い有効なプライオリティにされます。

Syntax

```
spanning-tree mst priority <0-4094> <0-61440>
no spanning-tree mst priority <0-4094>
```

<0-4094> - マルチプルスパニングツリーインスタンスID

<0-61440> - プライオリティ値(範囲 0～61440)

no - このコマンドは特定のマルチプルスパニングツリーインスタンスについてのブリッジプライオリティをデフォルトすなわち 32768 に設定されます。<0-4094>のインスタンスは希望する既存マルチプルスパニングツリーインスタンスへ対応する番号です。

(デフォルトCIST IDと定義された)0 が<0-4094>として設定されれば、このコマンドは共通する内部のスパニングツリーのためのブリッジプライオリティパラメータをデフォルトすなわち 32768 に設定します 。

初期設定

32768

コマンド･モード

グローバル･コンフィグ

このコマンドはマルチプルスパニングツリーインスタンスとVLANの間に関連性を追加します。VLANはそれ以降は共通する内部スパニングツリーには関連付けられなくなります。 <0-4094>のインスタンスは希望する既存マルチプルスパニングツリーインスタンスに対応する数字です。<1-4094>は現在のVLAN IDに対応します。

Syntax
spanning-tree mst vlan <0-4094> <1-4094> no spanning-tree mst vlan <0-4094> <1-4094>

<0-4094> - マルチプルスパニングツリーインスタンスID

<1-4094> - VLAN ID (Range: 1 – 4094).

no - このコマンドはマルチプルスパニングツリーインスタンスとVLANとの関連性を削除します。VLANは共通する内部スパニングツリーに再度関連付けられます。<0-4094>のインスタンスは必要な既存マルチプルスパニングツリーインスタンスに対応する数字です。<1-4094>は現在のVLAN IDに対応します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドはマルチプルスパニングツリーインスタンス内または共通する内部スパニングツリーにおけるこのポートのパス･コスト、ポートプライオリティ、または外部パス･コストを設定します。<0-4094>パラメータが現在のマルチプルスパニングツリーインスタンスに対応します。そのマルチプルスパニングツリーインスタンスに対して構成されます。しかし、

(デフォルトのCIST IDに定義された)0 が<0-4094>として設定された場合、そのときは構成は共通する内部スパニングツリーインスタンスに対して実施されます 。

「コスト」のトークン信号が特定されれば、このコマンドは、<0-4094>パラメータにしたがって、マルチプルスパニングツリーインスタンスまたは共通する内部スパニングツリーインスタンス内のこのポートへのパス･コストを設定します。パス･コストは 1 から 200000000 自動の範囲の数字か自動で特定できます。「自動」が特定されている場合、パス･コスト値はリンク速度に基づいて設定されます。

Syntax
spanning-tree mst <0-4094> cost {<1-200000000> | auto} no spanning-tree mst <0-4094> cost

<0-4094> - マルチプルスパニングツリーインスタンスID

no - このコマンドはマルチプルスパニングツリーインスタンス内か共通する内部スパニングツリーにおけるこのポートへのパス･コストを各デフォルト値に設定します。<0-4094>のパラメータが現在のマルチプルスパニングツリーインスタンスに対応し、構成はそのマルチプルスパニングツリーインスタンスに対してなされます。しかし(デフォルトCIST IDに定義された)0 が<0-4094>として設定された場合、構成は共通する内部スパニングツリーインスタンスに対して実施されます 。

「コスト」のトークン信号が特定されれば、このコマンドは、<0-4094>パラメータにしたがって、マルチプルスパニングツリーインスタンスまたは共通する内部スパニングツリーインスタンス内のこのポートへのパス･コストをデフォルト値に設定、すなわち、リンク速度に基づいたパス･コスト値に設定します。

初期設定

コスト － 自動

コマンド･モード

インターフェイス･コンフィグ

「ポートプライオリティ」のトークン信号が特定されている場合このコマンドは特定のマルチプルスパニングツリーインスタンスまたは共通する内部スパニングツリーインスタンスの内部でのこのポートへのプライオリティを<0-4094>パラメータにしたがって設定します。ポートプライオリティの値は 0 から 240 の範囲を 16 ずつ増える数字になる。

Syntax
spanning-tree mst <0-4094> port-priority <0-240> no spanning-tree mst <0-4094> port-priority

<0-4094> - マルチプルスパニングツリーインスタンスID

no - このコマンドはマルチプルスパニングツリーインスタンス内か共通する内部スパニングツリーにおけるこのポートへのポートプライオリティを各デフォルト値に設定します。<0-4094>のパラメータが現在のマルチプルスパニングツリーインスタンスに対応するならば、構成はそのマルチプルスパニングツリーインスタンスに対してなされます。しかし(デフォルトCIST IDに定義された)ゼロが<0-4094>として通れば、構成は共通する内部スパニングツリーインスタンスに対して実施されます。

「ポートプライオリティ」のトークン信号が特定されている場合このコマンドは特定のマルチプルスパニングツリーインスタンスまたは共通する内部スパニングツリーインスタンスの内部でのこのポートへのプライオリティを<0-4094>パラメータにしたがってデフォルトすなわち 128 に設定します。

初期設定

ポートプライオリティ: 128

コマンド・モード

インターフェイス・コンフィグ

「外部コスト」のトークン信号が特定されている場合このコマンドは特定のマルチプルスパニングツリーインスタンスまたは共通する内部スパニングツリーインスタンスの内部でのこのポートへのパス･コストを<0-4094>パラメータにしたがって設定します。パス･コストは 1 から 200000000 の範囲の数字かまたは自動で特定できます。、「自動」が特定されればパス･コスト値はリンク速度に基づいて設定されます。

Syntax
spanning-tree mst <0-4094> external-cost {<1-200000000> | auto} no spanning-tree mst <0-4094> external-cost

<0-4094> - マルチプルスパニングツリーインスタンスID

no - no - このコマンドはマルチプルスパニングツリーインスタンス内か共通する内部スパニングツリーにおけるこのポートへの外部パス･コストを各デフォルト値に設定します。<0-4094>のパラメータが現在のマルチプルスパニングツリーインスタンスに対応し、構成はそのマルチプルスパニングツリーインスタンスに対してなされます。しかし(デフォルトCIST IDに定義された)0 が<0-4094>で合致すれば、構成は共通する内部スパニングツリーインスタンスに適用されます。

「コスト」のトークン信号が特定された場合、このコマンドは、<0-4094>パラメータに従い、マルチプルスパニングツリーインスタンスまたは共通する内部スパニングツリーインスタンス内のこのポートへのパス･コストをデフォルト値に設定、すなわち、リンク速度に基づいたパス･コスト値に設定します。

初期設定

コスト: 自動

コマンド･モード

インターフェイス･コンフィグ

9.10.2.14 **spanning-tree port mode**

このコマンドはこのポートへの管理スイッチポートの状態を有効化します。

Syntax
spanning-tree port mode no spanning-tree port mode

no - このコマンドこのポートへの管理スイッチポートの状態を無効化します

初期設定

有効化

コマンド・モード

インターフェイスの構成

このコマンドはすべてのポートへの管理スイッチポートの状態を有効化します。

Syntax
spanning-tree port mode all no spanning-tree port mode all

all – すべてのインターフェイス

no - このコマンドはこのポートへの管理スイッチポートの状態を無効化します。

初期設定

有効化

コマンド・モード

グローバル・コンフィグ

9.10.2.15 **spanning-tree edgeport**

このコマンドはこのポートが共通する内部スパニングツリー内でのエッジポートだと指定します。これによりこのポートが遅延なく転送状態へ遷移することを可能にします 。

Syntax
spanning-tree edgeport no spanning-tree edgeport

no -このコマンドはポートが共通する内部スパニングツリー内でのエッジポートではないと指定します 。

初期設定

無効

コマンド・モード

インターフェイスの構成

9.11 ユーザアカウント管理コマンド

9.11.1 Showコマンド

9.11.1.1 show users

このコマンドにより設定ユーザ名およびその設定内容を表示します。このコマンドはRead・Write権限のあるユーザにのみ使用することができます。システム上でSNMPが使用可能な場合にのみSNMPv3 フィールドが表示されます。

Syntax
show users

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

User Name: シリアルポート、Telnet、Webにログインするユーザ名。 空白エントリに名前を入力してスイッチに新たなユーザーを追加できる。 ユーザ名には、最大 8 文字を使用することができます。大文字と小文字は区別されません。 Adminとguest2 人のユーザーが工場側デフォルト値として含まれている 。.

User Access Mode: (このモードは)オペレーターがスイッチ上の(Read・Write可モード)パラメータを変更することができるかまたはそれらを見る(読み取り専用モード)ことができるだけかを表示します。工場出荷デフォルトでは管理者はRead・Write可のアクセスを持ち、ゲストは読み取り専用アクセスを持っています。ひとりのRead・Write可ユーザーと 5 人までの読み取り専用ユーザーが許可されます。

SNMPv3 Access Mode: SNMPv3 アクセスモードを示します。**Read- Write**に設定されている場合、SNMPv3 ユーザはシステム上のパラメータを設定、検索することができます。**Read Only**に設定されている場合、SNMPv3 ユーザはパラメータ情報の検索のみを行うことができます。SNMPv3 アクセスモードは、CLIアクセスモードやWebアクセスモードとは異なります。

SNMPv3 Authentication: 特定のログインユーザに使用する認証プロトコルを示します。

SNMPv3 Encryption: 特定のログインユーザに使用する暗号化プロトコルを示します。

9.11.1.2 **show users authentication**

このコマンドによりすべてのユーザおよび認証ログイン情報を表示します。また、デフォルトユーザに割り当てられた認証ログインリストも表示します。

Syntax
show users authentication

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

User : この欄は認証ログインリストを割当てられたすべてのユーザーをリストします。

System Login:／システムログイン : login.この欄はシステムログイン のためにユーザーに割当てられた認証ログインリストを表示します。

802.1x: この欄は 802.1xポートセキュリティのためのユーザーに割当てられた認証ログインリストを表示します。

9.11.2 Configコマンド

9.11.2.1 username

このコマンドにより空き領域がある場合に新規ユーザ（アカウント）を追加します。アカウントの<username>には最大 8 文字を入力することができます。名前にはハイフン（-）およびアンダーライン （_） を含めた英数字を使用することができます。<username>は大文字と小文字では区別されません。

6 つのユーザ名を定義することができます。

このコマンドにより既存オペレータのパスワードを変更します。ユーザのパスワードは8文字以内です。ユーザ認証が許可された場合、または暗号化が有効である場合、パスワードは 8 文字の英数字にする必要があります。ユーザ名とパスワードは大文字と小文字では区別されません。パスワードを変更した場合、オペレータの前回のパスワードが要求されます。前回のパスワードがない場合はenterキーを押します。

Syntax
username <username> {password <0|7> <password> | nopassword} no username <username>

<username> -新規ユーザ名（範囲：最大 8 文字）

no - 前回作成したユーザ名を削除します。

注 ： 管理ユーザのアカウントを削除することはできません。

nopassword - このコマンドにより既存オペレータのパスワードを空白に設定します。 パスワードを変更した場合、オペレータの前回のパスワードが要求されます。前回のパスワードがない場合はEnterキーを押します

初期設定

No password

コマンド・モード

グローバル・コンフィグ

9.11.2.2 username snmpv3 authentication

このコマンドにより特定のログインユーザに使用する認証プロトコルを指定します。有効な認証プロトコルはnone、md5、shaです。md5 またはshaを指定した場合、ユーザのログインパスワードはsnmpv3 認証パスワードとして使用されます。<username>は、指定した認証プロトコルが使用されるログインユーザ名です。

Syntax
username snmpv3 authentication <username> {none | md5 | sha} no username snmpv3 authentication <username>

<username> - ログインユーザ名.

md5 - md5 による認証方法

sha - shaによる認証方法

none - 認証方法なし

no - このコマンドにより特定のログインユーザに使用する認証プロトコルをnoneに設定します。<username>は、指定した認証プロトコルが使用されるログインユーザ名です。

初期設定

No authentication

コマンド・モード

グローバル・コンフィグ

9.11.2.3 username snmpv3 encryption

このコマンドにより特定のログインユーザに使用する暗号化プロトコルおよびキーを指定します。有効な暗号化プロトコルはnoneまたはdesです。desプロトコルには、コマンド行で指定するkeyが必要となります。Keyは最大 16 文字となります。desプロトコルを指定したがキーを与えていない場合、キーを入力するよう要求されます。noneを指定した場合、キーを与える必要はありません。<username>は、指定した暗号化プロトコルが使用されるログインユーザ名です。

Syntax
username snmpv3 encryption <username> {none | des <0|7> <key>} no username snmpv3 encryption <username>

<username> - ログインユーザ名.

des - des暗号化プロトコル

none - 暗号化プロトコルなし

no - このコマンドにより暗号化プロトコルをnoneに設定します。 <username>は、指定した暗号化プロトコルが使用されるログインユーザ名です。

初期設定

No encryption

コマンド・モード

グローバル・コンフィグ

9.11.2.4 username defaultlogin

このコマンドにより未設定ユーザがシステムにログインを行う際、認証ログインリストをそのユーザに割り当てます。設定内容は、ユーザがローカルで設定された場合、特定ユーザに割り当てられた認証ログインリストで上書きされます。この値が設定されていない場合、ユーザはローカル認証のみで認証されます。

Syntax
username defaultlogin <listname>

<listname> - 認証ログインリスト

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.11.2.5 username login

このコマンドによりシステムログインに使用する特定の認証ログインリストを特定ユーザに割り当てます。<username>は設定済みの<username>、および<listname>は設定済みのログインリストである必要があります。

リモート認証が必要なログインリストがユーザに割り当てられた場合、認証が完了するまで、CLI、Web、telnetセッションからのインターフェイスへのアクセスはすべてブロックされます。

「管理者」ユーザーに関連付けられたログインリストはスイッチから偶発的に遮断されるのを防止するため変更がきかないものであることに注意してください。

Syntax
username login <user> <listname>

<user> - ログインユーザ名.

<listname> - 認証ログインリスト

初期設定

認証なし

コマンド・モード

グローバル・コンフィグ

9.12 LinkStateコマンド

9.12.1.1 show link state

このコマンドはリンクステートの情報を表示します。

Syntax
show link state

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

グループ: グループIDはグループIDの数字を表示します。

モード: 無効化または有効化する管理者モードあるいはそのモードではないか

アップ/ダウンポート: アップ/ダウンストリームポートのために指定されたインターフェイスのリスト

9.12.2 Configコマンド

このコマンドはリンク・ステートの管理者モードを有効化または無効化します。「リンク・ステート」を使えば管理者モードの冗長な機能を有効化でき、その機能を無効化するにはnoのコマンドを使います 。

Syntax
link state no link state

no - このコマンドリンク・ステートの管理者モードを無効化します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

このコマンドによりリンク・ステートのグループを作成するか無効にします。'link state group 'コマンドを使えばグループを作成、noのコマンドではグループを無効にます 。

Syntax
link state group no link state group <group id>

<group id> - リンク・ステートのグループID (範囲 1～32)

no –このコマンドはリンク・ステートのグループを無効にします 。

初期設定

0

コマンド・モード

グローバル・コンフィグ

このコマンドはリンク·ステートのグループを有効化または無効化します。「リンク·ステートのグループ、<group id>を有効化する」を使えば個々のグループを有効化できますし、noコマンドを使えばグループを無効にできます。

Syntax
link state group enable <group id> no link state group enable <group id>

<group id> - リンク·ステートのグループID (範囲 1~32)

no – このコマンドはリンク·ステートのグループを無効化します。

デフォルトセッティング

無効

コマンドモード

グローバル·コンフィグ

このコマンドはリンク·ステートグループにアップストリームまたはダウンストリームのポートを設定します。ポートを監視するように設定するためには'link state group <group id> upstream'(リンク·ステートのグループの<group id>をアップストリームに) を使います。

Syntax
link state group <group id> upstream link state group < group id> downstream

<group id> - リンク·ステートのグループID (範囲 1~32)

Upstream/ Downstream port(s) - アップ/ダウンストリームポート番号に指定されるインタ ーフェイスのリスト

デフォルトセッティング

無効

コマンドモード

グローバル·コンフィグ

9.13 port-backupコマンド

9.13.1 show port-backup

このコマンドはポートのバックアップ情報を表示します。

Syntax
show port-backup

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

グループ: グループIDはグループIDの数字を表示します。

モード: 無効化または有効化する管理者モードあるいはそのモードではないか

バック/アップポート: アップ/ダウンストリームポート番号のために指定されたインターフェイスのリスト

9.13.2 Configコマンド

このコマンドはポートバックアップグループを作成するまたは無効にします。グループを作成するには'port-backup group'(ポートバックアップグループ) を使います。グループを無効にはnoコマンドを使います 。

Syntax
port-backup group no port-backup group <group id>

<group id> - ポートバックアップグループID (範囲 1～32)

no – このコマンドはポートバックアップグループを無効にします 。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドはポートバックアップグループのためにアクティブなポートまたはバックアップポートを設定します。'port-backup group <group id> <active | backup>'(ポートバックアップグループ<group id><active|backup>) はポートをアクティブに構成したりバックアップポートに構成したりするようポートを設定します。

Syntax
port-backup group <group id> active no port-backup group <group id> active port-backup group <group id> backup no port-backup group <group id> backup

<group id> - ポートバックアップグループID (範囲 1～32)

no – このコマンドはポートバックアップグループからアクティブまたはバックアップのポートを削除します。

デフォルトセッティング

なし

コマンドモード

グローバル・コンフィグ

このコマンドはポートバックアップグループを有効化または無効化します。'port-backup group enable <group id>'(ポートバックアップグループで<group id>を有効化する)では個々のグループを有効化し、noコマンドを使えばグループを無効化します。

Syntax
port-backup group enable <group id> no port-backup group enable <group id>

<group id> - ポートバックアップグループID(範囲 1～32)

no – このコマンドはポートバックアップグループを無効化します。

デフォルトセッティング

無効

コマンドモード

グローバル･コンフィグ

9.14 SNTPコマンド

9.14.1 Showコマンド

9.14.1.1 show sntp

このコマンドによりSNTPクライアントの現在時刻および設定内容を表示し、ローカル時刻が正しく更新されているかを表示します。

Syntax
show sntp

初期設定

なし

コマンド・モード

ユーザ EXEC, 特権EXEC

表示メッセージ

Last Update Time: 最終時計更新時刻

Last Unicast Attempt Time: 最終転送クエリ時刻 (unicastモード)

Last Attempt Status : 最終SNTP要求 (unicastモード) または非要求メッセージ (broadcastモード) のステータス

Broadcast Count: 最終リブート以降SNTPクライアントが受信し処理した、非要求ブロードキャストメッセージの現在の数

Time Zone: 設定タイムゾーン

9.14.1.2 show sntp client

このコマンドによりSNTPクライアント設定を表示します。

Syntax
show sntp client

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Client Supported Modes: 対応しているSNTPモード (Broadcast、Unicast、Multicast)

SNTP Version SNTP バージョン : クライアントが対応しているSNTPの最新バージョン

Port : SNTPクライアントポート

Client Mode: 設定されているSNTPクライアントモード

Unicast Poll Interval: 2 の累乗によるSNTPクライアントの秒単位のポール間隔値

Poll Timeout (Seconds): SNTPクライアントの秒単位のポールタイムアウト値

Poll Retry: SNTPクライアントのポール再試行値

9.14.1.3 show sntp server

このコマンドにより設定SNTPサーバ、およびSNTPサーバの設定を表示します。

Syntax
show sntp server

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Server IP Address: 設定SNTPサーバのIPアドレス

Server Type: サーバのアドレスタイプ

Server Stratum: 最後に受信した有効パケットの、サーバの要求階層

Server Reference ID: 最後に受信した有効パケットの、サーバの参照時計識別子

Server Mode: SNTPサーバモード

Server Max Entries: 許可されるSNTPサーバの合計数

Server Current Entries: 設定SNTPの合計数

各設定サーバ:

IP address: 設定SNTPサーバのIPアドレス

Address Type: 設定SNTPサーバのアドレスタイプ

Priority: 設定サーバのIPプライオリティタイプ

Version: サーバのSNTPバージョン番号。unicastモードでサーバのクエリに使用するプロトコルバージョン

Port: サーバのポート番号

Last Attempt Time: 特定サーバの最終サーバ試行時刻

Last Update Status: 最終サーバがアップデートしたステータス

Total Unicast Requests: サーバへの要求数

Failed Unicast Requests: サーバからの失敗要求数

9.14.2 Configコマンド

9.14.2.1 sntp broadcast client poll-interval

このコマンドにより<poll-interval>の値が 6～16 となる場合に、2 の累乗によるSNTPブロードキャストクライアントのポール間隔を秒単位で設定します。

Syntax
sntp broadcast client poll-interval <poll-interval> no sntp broadcast client poll-interval

<poll-interval> - 範囲は 6～16

no - このコマンドによりSNTPブロードキャストクライアントのポール間隔をデフォルト値に戻します。

初期設定

デフォルト値は 6

コマンド・モード

グローバル・コンフィグ

9.14.2.2 sntp client mode

このコマンドによりSimple Network Time Protocol (SNTP) のクライアントモードを有効化し、broadcast、multicast、unicastモードのいずれかに設定します 。

Syntax
sntp client mode [broadcast | unicast | multicast] no sntp client mode

no - このコマンドによりSimple Network Time Protocol (SNTP) のクライアントモードを無効化します 。



SNTP IPv4 のマルチキャストアドレスは 224.0.1.1.です。

SNTP IPv6 のマルチキャストアドレスはff05::101.です。

IPv6 アドレスはbroadcastモードに対応していません。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.14.2.3 sntp client port

このコマンドによりSNTPクライアントポートIDと、ポーリング間隔を秒単位で設定します。

Syntax
sntp client port <portid> no sntp client port

<portid> - SNTPクライアントポートID、1〜65536

初期設定

デフォルトポートIDは 123

コマンド・モード

グローバル・コンフィグ

9.14.2.4 sntp unicast client poll-interval

このコマンドによりSNTPユニキャストクライアントのポール間隔を秒単位で設定します。

Syntax
sntp unicast client poll-interval <poll-interval> no sntp unicast client poll-interval

<poll-interval> - ポーリング間隔。値が 6〜10 の場合、2^(値) 秒となります。

no - このコマンドによりSNTPユニキャストクライアントのポール間隔をデフォルト値に戻します。

初期設定

デフォルト値は 6 である。

コマンド・モード

グローバル・コンフィグ

9.14.2.5 sntp unicast client poll-timeout

このコマンドによりSNTPユニキャストクライアントのポールタイムアウトを秒単位で設定します。

Syntax
sntp unicast client poll-timeout <poll-timeout> no sntp unicast client poll-timeout

< poll-timeout > - 秒単位のポーリングタイムアウト。範囲は 1～30

no - このコマンドによりSNTPユニキャストクライアントのポールタイムアウトをデフォルト値に戻します。

初期設定

デフォルト値は 5 である。

コマンド・モード

グローバル・コンフィグ

9.14.2.6 sntp unicast client poll-retry

このコマンドによりSNTPユニキャストクライアントのポール再試行を秒単位で設定します。

Syntax
sntp unicast client poll-retry <poll-retry> no sntp unicast client poll-retry

< poll-retry> -秒単位のポーリング再試行。範囲は 0～10

no - このコマンドによりSNTPユニキャストクライアントのポール再試行をデフォルト値に戻します。

初期設定

デフォルト値は 1 である。

コマンド・モード

グローバル・コンフィグ

9.14.2.7 sntp server

このコマンドによりサーバアドレスがIPアドレスまたはドメイン名、およびアドレスタイプがIPv4、IPv6、またはDNSとなる場合に、SNTPサーバ (最大 3 つ) を設定します。プライオリティの値を 1〜3、バージョンの値を 1〜4、ポートIDの値を 1〜65535 に、任意で設定することができます。

Syntax

```
sntp server <ipaddress/ipv6address/domain-name> <addresstype> [<1-3> [<version> [<portid>]]]
no sntp server remove <ipaddress/ipv6address/domain-name>
```

<ipaddress/ipv6address/domain-name> - SNTPサーバのIPアドレス。

<addresstype> - アドレスタイプはipv4、ipv6、dns。

<1-3> -範囲は 1〜3。

<version> -範囲は 1〜4。

<portid> - 範囲は 1〜65535。

no - This command deletes an server from the configured SNTP servers.

初期設定

なし.

コマンド・モード

グローバル・コンフィグ

9.14.2.8 sntp clock timezone

このコマンドはスイッチの内部クロックに時間ゾーンを設定します。

Syntax
sntp clock timezone <name> <0-12> <0-59> {before-utc | after-utc}

<name> - タイムゾーン名、通常は省略表記 (範囲：1～15 文字)

<0-12> - UTC前後の時間数 (範囲：0～12 時間)

<0-59> - UTC前後の分数 (範囲：0～59 分)

before-utc - UTC (東側) 前のローカルタイムゾーンを設定します。

after-utc - UTC (西側) 後のローカルタイムゾーンを設定します。

初期設定

Taipei 08:00 After UTC

コマンド・モード

グローバル・コンフィグ

9.14.2.9 sntp multicast client poll-internal

このコマンドによりSNTPマルチキャストクライアントのポール間隔を秒単位で設定します。

Syntax
sntp multicast client poll-interval <poll-interval> no sntp multicast client poll-interval

<poll-interval> - ポーリング間隔。値の範囲が 6～10 の場合、2^(値) 秒となります。

no – このコマンドによりSNTPマルチキャストクライアントのポール間隔をデフォルト値に戻します。

初期設定

デフォルト値は 6 である。

コマンド・モード

グローバル・コンフィグ

9.15 Securityコマンド

9.15.1 Showコマンド

9.15.1.1 show users authentication

このコマンドによりすべてのユーザおよび認証ログイン情報を表示します。また、デフォルトユーザに割り当てられた認証ログインリストも表示します。

Syntax
show users authentication

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

User: 認証ログインリストが割り当てられているすべてのユーザを列記します。

System Login: ユーザに割り当てられた、システムログインに使用する認証ログインリストを示します。

802.1x: ユーザに割り当てられた、802.1xポートセキュリティに使用する認証ログインリストを示します。

9.15.1.2 show authentication

このコマンドによりすべての認証ログインリストの順列認証メソッドを表示します。

Syntax
show authentication

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Authentication Login List: 認証ログインリスト名を示します。

Method 1: 特定の認証ログインリストに 1 つめのメソッドがあれば表示します。

Method 2: 特定の認証ログインリストに 2 つめのメソッドがあれば表示します。

Method 3: 特定の認証ログインリストに 3 つめのメソッドがあれば表示します。

9.15.1.3 show authentication users

このコマンドにより特定の認証ログインリストに割り当てられているユーザの情報を表示します。未設定のユーザにログインが割り当てられている場合、ユーザ列にユーザdefaultを表示します。

Syntax
show authentication users <listname>

<listname> - 認証ログインリスト名

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

User Name : 特定の認証ログインリストに割り当てられたユーザを表示します。

Component: 認証ログインリストが割り当てられているコンポーネント (Userまたは 802.1x) を表示します。

9.15.1.4 show dot1x

このコマンドによりdot1x Administrativeモードのステータスを表示します。

Syntax
show dot1x

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Administrative Mode: スイッチの認証コントロールを有効化するか無効化するかを表示します。

9.15.1.5 **show dot1x detail**

このコマンドにより特定ポートのグローバルdot1x設定の概要およびdot1x設定の詳細を表示します。

Syntax
show dot1x detail <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Port: 設定を表示するインターフェイス

Protocol Version: このポートに関連するプロトコルバージョン。dot1x仕様の最初のバージョンに対応するため、値は 1 となります。

PAE Capabilities: このポートのポートアクセスエンティティ (PAE) の機能。値はAuthenticatorまたはSupplicant

Authenticator PAE State: 認証者PAE状態マシンの現在の状態。値はInitialize、Disconnected、Connecting、Authenticating、Authenticated、Aborting、Held、ForceAuthorized、ForceUnauthorized

Backend Authentication State: バックエンド認証状態マシンの現在の状態。値はRequest、Response、Success、Fail、Timeout、Idle、Initialize

Quiet Period: サプリカントの取得を試行しない時間を定義するための、このポート上の認証者状態マシンで使用する時間。値は秒数で表示され、範囲は 0～65535 です 。

Transmit Period: サプリカントへEAPOL EAP Request/Identityフレームを送信するタイミングを決定するための、特定ポート上の認証者状態マシンで使用するタイマー。値は秒数で表示され、範囲は 1～65535 です。

Supplicant Timeout: サプリカントをタイムアウトにするための、このポート上の認証者状態マシンで使用するタイマー。値は秒数で表示され、範囲は 1～65535 です。

Server Timeout: 認証サーバをタイムアウトにするための、このポート上の認証者で使用するタイマー。値は秒数で表示され、範囲は 1～65535 です。

Maximum Requests: サプリカントをタイムアウトにする前に、このポート上の認証者状態マシンがEAPOL EAP Request/Identityを再送する最大回数。値の範囲は 1～10

Reauthentication Period: サプリカントの再認証実施を決定するための、このポート上の認証者状態マシンで使用するタイマー。 値は秒数で表示され、範囲は 1～65535 です。

Reauthentication Enabled: このポートで再認証が有効であるかを示します。値はTrueまたはFalse

Key Transmission Enabled: 特定ポートのサプリカントへキーを送信するかを示します。値はTrueまたはFalse

Control Direction: 特定ポートまたは複数ポートの制御方向を示します。値はbothまたはin

9.15.1.6 show dot1x statistics

このコマンドにより特定ポートのグローバルdot1x設定の概要およびdot1x統計データを表示します。

Syntax
show dot1x statistics <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Port: 統計データを表示するインターフェイス

EAPOL Frames Received: この認証符号で受信した、いずれかのタイプの有効EAPOLフレームの数

EAPOL Frames Transmitted : この認証符号で送信した、いずれかのタイプのEAPOLフレームの数

EAPOL Start Frames Received: この認証符号で受信した、EAPOL開始フレームの数

EAPOL Logoff Frames Received: この認証符号で受信した、EAPOLログオフフレームの数

Last EAPOL Frame Version: 最後に受信したEAPOLフレームのプロトコルバージョン番号

Last EAPOL Frame Source: 最後に受信したEAPOLフレームのソースMACアドレス

EAPOL Response/Id Frames Received: この認証符号で受信したEAP response/identityフレームの数

EAP Response Frames Received: この認証符号で受信した有効EAP responseフレームの数

EAP Request/Id Frames Transmitted: この認証符号で送信したEAP request/identityフレームの数

EAP Request Frames Transmitted: この認証符号で送信したEAP requestフレーム (request/identityフレームより古いもの) の数

Invalid EAPOL Frames Received: フレームタイプが識別されていない認証符号で受信した、EAPOLフレームの数

EAP Length Error Frames Received: フレームタイプが識別されていない認証符号で受信した、EAPOLフレームの数

9.15.1.7 show dot1x summary

このコマンドにより特定ポートまたはすべてのポートの、グローバルdot1x設定の概要およびdot1x設定の概要を表示します。

Syntax
show dot1x summary {<slot/port> | all}

<slot/port> - 必要なインターフェイス番号である。

all - すべてのインターフェイス。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Interface: 設定を表示するインターフェイス。

Control Mode: このポートの設定制御モード。値はforce-unauthorized、force-authorized、auto

Operating Control Mode: このポートが動作する制御モード。値はauthorized、unauthorized

Reauthentication Enabled: このポートで再認証が有効であるかを示します。

Port Status: 特定ポートのサプリカントへキーを送信するかを示します。

9.15.1.8 show dot1x users

このコマンドによりローカルで設定されたユーザの 802.1xポートセキュリティユーザ情報を表示します。

Syntax
show dot1x users <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

User: 特定ポートへのアクセス権をローカルで設定されたユーザ

9.15.1.9 show radius-servers

このコマンドにより設定したRADIUSサーバの項目を表示します。

Syntax
show radius-servers

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

IP Address: 設定したRADIUSサーバのIPアドレス

Port: このサーバで使用しているポート

Type: Primaryまたはsecondary

Secret Configured: Yes / No Message Authenticator: RADIUSサーバに設定された、メッセージ認証符号の属性

9.15.1.10 show radius

このコマンドによりIBPにおけるRADIUSのさまざまな設定項目を表示します。

Syntax
show radius

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Current Server Host Address : 現在、認証に使用している設定サーバ

Number of Configured Servers: 認証サーバの設定IPアドレス

Number of retransmits: 要求パケットが再送される最大回数の設定値

Timeout Duration: 要求の再送を行う秒単位の設定タイムアウト値

RADIUS Accounting Mode: DisableまたはEnabled

RADIUS Dead Time: RADIUSサーバがダウンした場合の設定復帰時間

RADIUS Attribute 4 Mode: RADIUS NAS-IP属性を有効化または無効化します。

RADIUS Attribute 4 Value: RADIUS NAS-IP値

9.15.1.11 show radius accounting

このコマンドにより設定RADIUSアカウンティングモード、アカウンティングサーバ、設定アカウンティングサーバの統計データを表示します。

Syntax
show radius accounting [statistics <ipaddr|hostname>]

<ipaddr|hostname> - IPアドレスまたはホスト名

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

任意のトークン「statistics <ipaddr|hostname>」が含まれていない場合、アカウンティングモード、およびRADIUSアカウンティングサーバ詳細情報のみが表示されます。

RADIUS Accounting Mode: Enabledまたはdisabled

Host Address: RADIUSアカウンティングサーバの設定値

Port : RADIUSアカウンティングサーバで使用されているポート

Secret Configured: YesまたはNo

任意のトークン「statistics <ipaddr|hostname>」が含まれている場合、設定RADIUSアカウンティングサーバの統計が表示されます。表示されるRADIUSアカウンティングサーバの統計データは以下のとおりです。

RADIUS Accounting Server Host Address: 設定RADIUSアカウンティングサーバのホストアドレス値

Round Trip Time: 最新のAccounting- Responseと、RADIUSアカウンティングサーバからのAccounting-Requestと一致するAccounting-Request間の、センチ秒単位の時間間隔

Requests: このアカウンティングサーバに送信された、RADIUS Accounting-Requestパケット数。ただし再送分は含まれません。

Retransmission: RADIUSアカウンティングサーバに再送された、RADIUS Accounting-Requestパケット数。

Responses: アカウンティングポート上で受信した、このサーバからのRADIUSパケット数。

Malformed Responses: このサーバから受信した、異常RADIUS Accounting-Responseパケット数。異常パケットには、無効な長さのパケットも含まれます。ただし、不正な認証符号および不明なタイプは、異常アカウンティング応答には含まれません。

Bad Authenticators: このアカウンティングサーバから受信した、無効な認証符号のあるRADIUS Accounting-Responseパケット数

Pending Requests: タイムアウトとなっていない、または応答を受信していない、このサーバへ送信されたRADIUS Accounting-Requestパケット数

Timeouts: このサーバへのアカウンティングタイムアウト数

Unknown Types: アカウンティングポートのサーバから受信した、不明タイプのRADIUSパケット数

Packets Dropped: アカウンティングポートのサーバから受信し、なんらかの理由によりドロップされたRADIUSパケット数

9.15.1.12 show radius statistics

このコマンドによりRADIUSまたは設定サーバの統計データを表示します。設定RADIUSサーバの統計データを表示するには、指定したIPアドレスが前回設定したRADIUSサーバのIPアドレスと一致する必要があります。実行すると以下のフィールドが表示されます。

Syntax
show radius statistics <ipaddr|hostname>

<ipaddr|hostname> - IPアドレスまたはホスト名。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Server Host Address: サーバのIPアドレスまたはホスト名

Round Trip Time: 最新のAccess-Reply/ Access-Challengeと、RADIUS認証サーバからのAccounting-Requestと一致するAccounting-Request間の、100 分の 1 秒単位の時間間隔

Access Requests: このサーバに送信されたRADIUS Access-Requestパケット数。ただし、再送分は含まれません。

Access Retransmission: このRADIUS認証サーバに再送された、RADIUS Access-Requestパケット数。

Access Accepts: このサーバから受信した、有効パケットと無効パケットを含むRADIUS Access-Acceptパケット数。

Access Rejects: このサーバから受信した、有効パケットと無効パケットを含むRADIUS Access-Rejectパケット数。

Access Challenges: このサーバから受信した、有効パケットと無効パケットを含むRADIUS Access-Challengeパケット数。

Malformed Access Responses: このサーバから受信した、異常RADIUS Access-Responseパケット数。異常パケットには、無効な長さのパケットも含まれます。ただし、不正な認証符号やシグネチャ属性、または不明なタイプは、異常アクセス応答には含まれません。

Bad Authenticators: このサーバから受信した、無効な認証符号またはシグネチャ属性を含む、RADIUS Access-Responseパケット数。

Pending Requests: タイムアウトとなっていない、または応答を受信していない、このサーバへ送信されるRADIUS Access-Requestパケット数

Timeouts: このサーバへの認証タイムアウト数

Unknown Types:認証ポートのサーバから受信した、不明タイプのRADIUSパケット数

Packets Dropped: 認証ポートのサーバから受信し、なんらかの理由によりドロップされたRADIUSパケット数

9.15.1.13 show tacacs

このコマンドによりTACACSの設定情報を表示します。

Syntax
show tacacs

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Global Timeout: すべてのサーバのTACACSのグローバルタイムアウト値を示します。

IP Address: TACACSサーバ

Port: TACACS packet port number

Timeout (sec): TACACSサーバが応答を行わない間の、秒単位のタイムアウト値

Priority: サーバプライオリティ (0 は最高プライオリティ)

9.15.1.14 show port-security

このコマンドによりシステム全体のポートセキュリティ設定を表示します。

Syntax
show port-security

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Port Security Administration Mode: システム全体のポートロックモード

このコマンドにより特定のインターフェイスまたはすべてのインターフェイスのポートセキュリティ設定を表示します。

Syntax
show port-security { <slot/port> | all }

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Intf: インターフェイス番号

Admin Mode: インターフェイスのポートロックモード

Dynamic Limit: 動的に割り当てるMACアドレスの最大数

Static Limit: 静的に割り当てるMACアドレスの最大数

Violation Trap Mode: バイオレーショントラップが有効であるかを示します 。

Violation Shutdown: バイオレーションシャットダウンが有効であるかを示します 。

このコマンドにより動的にロックされた、ポートのMACアドレスを表示します。

Syntax
show port-security dynamic <slot/port>

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

MAC Address: 動的にロックされたMACアドレス

このコマンドにより静的にロックされた、ポートのMACアドレスを表示します。

Syntax
show port-security static <slot/port>

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

MAC Address: 静的にロックされたMACアドレス

このコマンドによりロックされたポート上で破棄された最終パケットのソースMACアドレスを表示します。

Syntax
show port-security violation <slot/port>

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

MAC address: ロックされたポート上で破棄されたパケットのMACアドレス

9.15.2 Configコマンド

9.15.2.1 authentication login

このコマンドにより認証ログインリストを作成します。<listname>には、大文字と小文字で区別されない最大 15 文字の英数字を入力します。IBPで、最大 10 個の認証ログインリストを設定することができます。リストを作成すると、認証メソッド local が最初のメソッドに設定されます。

任意のパラメータ method1、 method 2、 method 3 のすべてまたはいずれかを使用した場合、メソッドの順列リストが認証ログインリスト内に設定されます。認証ログインリストがない場合、新規の認証ログインリストが作成された後、認証ログインリストに認証メソッドが設定されます。認証ログインメソッドは最大 3 つです。メソッドの値は、local、radius、reject、tacacsです。

localは、ローカルで保存されたユーザIDおよびパスワードが認証に使用されること、radiusは、ユーザIDとパスワードがRADIUSサーバを使用して認証されること、rejectは、ユーザ認証を行わないこと、tacacsは、ユーザIDとパスワードがTACACSを使用して認証されることを示します。

ユーザ認証では、認証試行が成功または失敗するまでユーザログインで認証メソッドを順番に試行します。

注記：デフォルト設定が含まれているデフォルトログインリストの内容は変更できません。

Syntax
authentication login <listname> [<method1>] [<method2>] [<method3>] no authentication login <listname>

<listname> - 認証ログインリストを作成します（範囲：最大 15 文字）

<method1 - 3> - メソッド値は local、radius、reject、tacacs

no - このコマンドにより特定の認証ログインリストを削除します。以下いずれかの条件がtrueの場合、削除は失敗となります。

ログインリスト名が無効である、または既存の認証ログインリストと一致しない。

特定の認証ログインリストがいずれかのユーザ、あるいはいずれかのコンポーネントの非設定ユーザに割り当てられている。

ログインリストが、デフォルト設定の含まれたデフォルトログインリストであり、「config authentication login create」を使用して作成されていない。デフォルトログインリストの削除はできません。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.15.2.2 username defaultlogin

このコマンドによりシステムへのログイン試行に使用する認証ログインリストを、非設定ユーザに割り当てます。この設定は、ユーザがローカルで設定されている場合、特定ユーザに割り当てられた認証ログインリストで上書きされます。この値が設定されていない場合、ユーザはローカル認証のみで認証されます。

Syntax
username defaultlogin <listname>

<listname> - 認証ログインリスト

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.15.2.3 username login

このコマンドによりシステムログインに使用する特定の認証ログインリストを特定のユーザに割り当てます。<username>は設定された<username>、<listname>は設定されたログインリストである必要があります。

リモート認証が必要なログインリストがユーザに割り当てられている場合、すべてのCLI、web、telnetからのインターフェイスへのアクセスはすべて、認証が完了するまでブロックされます。

'admin' ユーザーに関連付けられたログインリストはスイッチから偶発的に遮断されるのを防止するため変更できないことに注意しましょう。

Syntax
username login <user> <listname>

<user> - ログインユーザ名.

<listname> - 認証ログインリスト

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.15.3 Dot1xコマンド

9.15.3.1 dot1x initialize

このコマンドにより特定ポートの初期化シーケンスを開始します。このコマンドは、特定ポートの制御モードが「auto」の場合のみ有効化されます。制御モードが「auto」でない場合、エラーが返されます。

Syntax
dot1x initialize <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

特権EXEC

9.15.3.2 dot1x default-login

このコマンドにより認証ログインリストを、802.1xポートセキュリティの非設定ユーザに割り当てます。この設定は、ユーザがローカルで設定されている場合、特定ユーザに割り当てられた認証ログインリストで上書きされます。この値が設定されていない場合、ユーザはローカル認証のみで認証されます。

Syntax
dot1x defaultl-login <listname>

<listname> - 認証ログインリスト

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.15.3.3 dot1x login

このコマンドにより特定の認証ログインリストを、802.1xポートセキュリティの特定ユーザに割り当てます。<user>パラメータは設定済みユーザ、<listname>パラメータは設定済み認証ログインリストである必要があります。

Syntax
dot1x login <user> <listname>

<user> - ログインユーザ名.

<listname> - 認証ログインリスト

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.15.3.4 dot1x system-auth-control

このコマンドはスイッチのdot1x認証サポートを有効化するために使われます。デフォルトで認証対応は無効となっています。無効に設定されているとdot1x設定は保持され、変更することができますが、アクティブにすることはできません。

Syntax
dot1x system-auth-control no dot1x system-auth-control

no - このコマンドはスイッチのdot1x認証サポートを無効化するために使われます。

初期設定

Disabled

コマンド･モード

グローバル･コンフィグ

9.15.3.5 dot1x user

このコマンドにより特定ポートまたはすべてのポートへのアクセス権をもつユーザのリストに、特定ユーザを追加します。<username>パラメータは設定済みユーザである必要があります。

Syntax
dot1x user <user> {<slot/port> | all} no dot1x user <user> {<slot/port> | all}

<user> - ログインユーザ名.

<slot/port> - 必要なインターフェイス番号である。

all - すべてのインターフェイス。

no - このコマンドにより特定ポートまたはすべてのポートへのアクセス権をも つユーザのリストからそのユーザを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.15.3.6 dot1x port-control

このコマンドによりすべてのポートに使用する認証モードを設定します。制御モードは以下のいずれかとなります。

force unauthorized: 認証者PAEで、制御ポートを無条件で非認証に設定します。

force authorized: 認証コード・ポート・アクセス・エンティティ (PAE)は制御されるポートを無条件に認証に設定する。

auto: 認証コードPAEはポート・モードを認証請求者、認証コード、および認証サーバの間の認証交換結果を反映するうに設定する。

Syntax
dot1x port-control all {auto | force-authorized | force-unauthorized} no dot1x port-control all

all - すべてのインターフェイス。

no - このコマンドによりすべてのポートで使用する認証モードを「auto」に設定します。

初期設定

auto

コマンド・モード

グローバル・コンフィグ

このコマンドにより使用する認証モードを特定ポートに設定します。制御モードは以下のいずれかとなります。

force unauthorized: 認証者PAEで、制御ポートを無条件で非認証に設定します。

force authorized: 認証コード・ポート・アクセス・エンティティ（PAE)は制御されるポートを無条件に認証に設定する。

auto: 認証コードPAEはポート・モードを認証請求者、認証コード、および認証サーバの間の認証交換結果を反映するうに設定する。

Syntax
dot1x port-control {auto | force-authorized | force-unauthorized} no dot1x port-control

no - このコマンドにより特定ポートで使用する認証モードを「auto」に設定します。

初期設定

auto

コマンド・モード

インターフェイス・コンフィグ

9.15.3.7 dot1x max-req

このコマンドによりサプリカントをタイムアウトするまでにポート上の認証者状態マシンがEAPOL EAP Request/Identityフレームを送信する最大回数を設定します。<1-10>の値は 1～10 の範囲となります。

Syntax
dot1x max-req <1-10> no dot1x max-req

<1-10> -最大回数（範囲：1～10）

no - このコマンドによりサプリカントをタイムアウトするまでにポート上の認証者状態マシンがEAPOL EAP Request/Identityフレームを送信する最大回数を、デフォルト値の 2 に設定します。

初期設定

2

コマンド・モード

インターフェイス・コンフィグ

9.15.3.8 dot1x re-authentication

このコマンドにより特定ポートのサプリカントの再認証を有効化します。

Syntax
dot1x re-authentication no dot1x re-authentication

no - このコマンドにより特定ポートのサプリカントの再認証を無効化します。

初期設定

Disabled

コマンド・モード

インターフェイス・コンフィグ

9.15.3.9 dot1x re-reauthenticate

このコマンドにより特定ポートの再認証シーケンスを開始します。このコマンドは、特定ポートの制御モードが「auto」の場合のみ有効化されます。制御モードが「auto」でない場合、エラーが返されます。

Syntax
dot1x re-authenticate <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

特権EXEC

9.15.3.10 **dot1x timeout**

このコマンドによりポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定します。使用しているトークンおよび送信された値(秒単位)により、異なるタイムアウト設定可能パラメータが設定されます。以下のトークンに対応しています。

reauth-period: ポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定し、サプリカントの再認証を行うタイミングを決定します。reauth-periodの値は 1～65535 である必要があります。

quiet-period: ポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定し、サプリカントの取得を行わない時間を定義します。quiet-periodの値は 1～65535 である必要があります。

tx-period: ポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定し、サプリカントへEAPOL EAP Request/Identityフレームを送信するタイミングを決定します。quiet-periodの値は 1 ~ 65535 である必要があります。

supp-timeout: ポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定し、サプリカントをタイムアウトします。supp-timeoutの値は 1～65535 である必要があります。

server-timeout: ポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定し、認証サーバをタイムアウトします。supp-timeoutの値は 1 - 65535 である必要があります。

Syntax
dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period} <seconds> no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period}

<seconds> - 値の範囲は 1～65535

no – このコマンドによりポートの認証者状態マシンで使用されている秒単位のタイマーの値を、デフォルト値に設定します。使用しているトークンに該当するデフォルト値が設定されます。

初期設定

reauth-period: 3600 秒

quiet-period: 60 秒

tx-period: 30 秒

supp-timeout: 30 秒

server-timeout: 30 秒

コマンド・モード

インターフェイス・コンフィグ

9.15.4 Radiusコマンド

9.15.4.1 radius accounting mode

このコマンドによりRADIUSアカウンティング機能を有効化します。

Syntax
radius accounting mode no radius accounting mode

no - このコマンドによりRADIUSアカウンティング機能をデフォルト値に設定します。つまり、RADIUSアカウンティング機能が無効となります。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

9.15.4.2 radius-server host

このコマンドによりRADIUS認証サーバおよびRADIUSアカウンティングサーバを設定します。

「auth」トークンを使用している場合、このコマンドによりRADIUS認証サーバへの接続に使用するIPアドレスを設定します。1 つのRADIUSクライアントあたり最大 3 つのサーバを設定することができます。設定サーバが最大数になると、noコマンドを実行しサーバが 1 つ削除されるまで、このコマンドは失敗となります。任意の<port>パラメータを使用している場合、このコマンドにより設定RADIUSサーバへの接続に使用するUDPポート番号を設定します。UDPポート番号を設定するには、IPアドレスが、前回設定されたRADIUS認証サーバのIPアドレスと一致する必要があります。ポート番号の範囲は 1～65535、デフォルト値は 1812 です。

「acct」トークンを使用している場合、このコマンドによりRADIUSアカウンティングサーバに使用するIPアドレスを設定します。アカウンティングサーバは 1 つのみ設定できます。アカウンティングサーバが現在設定されている場合、このコマンドが成功する前に、noコマンドを使用し設定からそのサーバを削除する必要があります。任意の<port>パラメータを使用している場合、このコマンドによりRADIUSアカウンティングサーバへの接続に使用するUDPポートを設定します。指定したIPアドレスは、前回設定されたアカウンティングサーバのIPアドレスと一致する必要があります。ポートがすでにアカウンティングサーバに設定されている場合、前回設定された値が新規ポートで置き換えられます。ポート値の範囲は 1～65535、デフォルト値は 1813 です。

Syntax
radius-server host {acct | auth} <ipaddr|hostname> [port] no radius-server host {acct | auth} <ipaddr|hostname>

<ipaddr|hostname> - IPアドレスまたはホスト名。

[port] - ポート番号 (範囲：1～65535)

no - このコマンドにより設定RADIUS認証サーバまたはRADIUSアカウンティングサーバを削除します。「auth」

トークンを使用している場合、前回設定されたRADIUS認証サーバが設定から削除されます。同様に、「acct」トークンを使用している場合、前回設定されたRADIUSアカウンティングサーバが設定から削除されます。<ipaddr|hostname>パラメータは、前回設定されたRADIUS認証サーバまたはRADIUSアカウンティングサーバのIPアドレスまたはホスト名と一致する必要があります。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.15.4.3 radius-sever key

このコマンドによりRADIUSクライアントと、RADIUS認証サーバまたはRADIUSアカウンティングサーバ間の共有鍵を設定します。使用しているトークンが「auth」か「acct」であるかによって、共有キーがRADIUS認証サーバまたはRADIUSアカウンティングサーバに設定されます。与えられたIPアドレスは、前回設定したサーバのIPアドレスと一致する必要があります。このコマンドを実行すると、共有キーを入力するよう表示されます。共有キーは 20 文字以内の英数字となります 。

Syntax
radius-server key {acct | auth} <ipaddr|hostname> <0|7> <key-value>

<ipaddr|hostname> - IPアドレスまたはホスト名

<0|7> - 0 はプレーンテキスト形式のキー、7 は暗号化形式のキーを示します。

<key-value> -共有キー 。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.15.4.4 radius-server retransmit

このコマンドによりRADIUSサーバから応答を受信しなかった場合に要求パケットを再送する最大回数を設定します。再試行の値は 1～15 の整数となります。

Syntax
radius-server retransmit <retries> no radius-server retransmit

<retries> -最大回数（範囲：1～15）

no - このコマンドによりRADIUSサーバから応答を受信しなかった場合に要求パケットを再送する最大回数を、デフォルト値の 10 に設定します。

初期設定

10

コマンド・モード

グローバル・コンフィグ

9.15.4.5 radius-server timeout

このコマンドにより応答を受信しなかった場合にRADIUSサーバに要求を再送した後のタイムアウト値を秒単位で設定します。タイムアウト値は 1～30 の整数となります。

Syntax
radius-server timeout <seconds> no radius-server timeout

<seconds> -最大タイムアウト（範囲：1～30）

no - このコマンドにより応答を受信しなかった場合にRADIUSサーバに要求を再送した後の秒単位のタイムアウト値を、デフォルト値の 6 に設定します。

初期設定

6

コマンド・モード

グローバル・コンフィグ

9.15.4.6 radius-server msgauth

このコマンドにより特定サーバのメッセージ認証符号属性を有効化します。

Syntax
radius-server msgauth <ipaddr|hostname>

<ipaddr|hostname> - IPアドレスまたはホスト名

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.15.4.7 radius-server primary

このコマンドによりRADIUSクライアントにプライマリRADIUS認証サーバを設定します。プライマリサーバは、RADIUS要求の処理に使用するようデフォルトで設定されているものです。残りの設定サーバは、プライマリサーバにアクセスできない場合にのみ使用されます。最大 3 つのサーバを各クライアントに設定することができます。このうち1つのサーバのみをプライマリとして設定することができます。プライマリサーバがすでにこのコマンドの実行前に設定されている場合、このコマンドで使用されるIPアドレスで指定されたサーバが新規のプライマリサーバとなります。IPアドレスは、前回設定されたRADIUS認証サーバのIPアドレスと一致する必要があります。

Syntax
radius-server primary <ipaddr|hostname>

<ipaddr|hostname> - IPアドレスまたはホスト名

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.15.5 TACACS+コマンド

9.15.5.1 tacacs host

このコマンドによりTACACSサーバを設定します。

このコマンドを実行すると、コマンドモードがTACACSモードに変更され、指定した値をホストに設定します。

Syntax
tacacs host <ipaddr|hostname> no tacacs host <ipaddr|hostname>

<ipaddr|hostname> - IPアドレスまたはホスト名

no - このコマンドにより設定したTACACSサーバを削除します。<ipaddr|hostname>パラメータは、前回設定したTACACSサーバのIPアドレスまたはホスト名と一致する必要があります。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりTACACSサーバの設定認証および暗号化キーを設定します。

Syntax
key [<0/7> <key-value>]

このコマンドにパラメータがない場合、キーの値は削除され、グローバルキーが使用されます。

注記：共有鍵は最大 32 文字です。

<0/7> - 0 はプレーンテキスト形式のキー、7 は暗号化形式のキーを示します。.

<key-value> - TACACS認証および暗号化キー

初期設定

なし

コマンド・モード

TACACSモード

このコマンドによりTACACSサーバのサービスポートを設定します。

Syntax
port [<0-65535>]

このコマンドにパラメータがない場合、ポートの値がデフォルト値に戻ります。

<0-65535> - TACACSサービスポート (範囲：0～65535)

初期設定

49

コマンド・モード

TACACSモード

このコマンドによりTACACSサーバのプライオリティを設定します。

Syntax
Priority [<0-65535>]

このコマンドにパラメータがない場合、プライオリティの値がデフォルト値に戻ります。

<0-65535> - TACACSサービスのプライオリティ (範囲：0～65535)

初期設定

0

コマンド・モード

TACACSモード

このコマンドによりTACACSの指定接続タイムアウト値を設定します。

Syntax

```
timeout [<seconds>]
```

このコマンドにパラメータがない場合、タイムアウト値は削除され、グローバルタイムアウトが使用されます。

<seconds> - TACACSの接続タイムアウト値 (範囲：1～30)

初期設定

なし

コマンド・モード

TACACSモード

9.15.5.2 tacacs key

このコマンドによりTACACSサーバのグローバル認証および暗号化キーを設定します。

Syntax

```
tacacs key <0/7> <key-value>
no tacacs key
```

注記：共有鍵は最大 32 文字です。

<0/7> - 0 はプレーンテキスト形式のキー、7 は暗号化形式のキーを示します。.

<key-value> - TACACS認証および暗号化キー

no - このコマンドによりTACACSサーバ共有鍵を削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.15.5.3 tacacs timeout

このコマンドによりTACACSのグローバル接続タイムアウト値を設定します。

Syntax
tacacs timeout <seconds> no tacacs timeout

<seconds> - TACACSの接続タイムアウト値（範囲：1～30）。

no - このコマンドによりタイムアウト値をデフォルト値に戻します。

初期設定

5

コマンド・モード

グローバル・コンフィグ

9.15.6 port-securityコマンド

9.15.6.1 port-security

このコマンドによりシステムレベル (グローバル･コンフィグ) またはポートレベル (Interface Config) のポートロックを有効化します。

Syntax
port-security no port-security

初期設定

なし

コマンド･モード

グローバル･コンフィグ、インターフェイス･コンフィグ

9.15.6.2 port-security max-dynamic

このコマンドにより動的にロックされたMACアドレスを特定ポートに許可する最大数を設定します。

Syntax
port-security max-dynamic [<0-600>] no port-security max-dynamic

no - このコマンドにより動的にロックされたMACアドレスを特定ポートに許可する最大数をデフォ ルト値 に戻します。

初期設定

600

コマンド･モード

インターフェイス･コンフィグ

9.15.6.3 port-security max-static

このコマンドにより静的にロックされたMACアドレスを特定ポートに許可する最大数を設定します。

Syntax
port-security max-static [<0-20>] no port-security max-static

no - このコマンドにより静的にロックされたMACアドレスを特定ポートに許可する最大数をデ フォルト 値に戻します。

初期設定

20

コマンド・モード

インターフェイス・コンフィグ

9.15.6.4 port-security mac-address

このコマンドにより静的に登録されたMACアドレスのリストにMACアドレスを追加します 。

Syntax
port-security mac-address <mac-addr> <1-4094> no port-security mac-address <mac-addr> <1-4094>

<1-4094> - VLAN ID

<mac-addr> -静的MACアドレス

no -このコマンドにより静的に登録されたMACアドレスのリストからMACアドレスを削除します 。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

9.15.6.5 port-security mac-address move

このコマンドにより動的にロックされたMACアドレスを、静的に登録されたMACアドレスに変換します 。

Syntax
port-security mac-address move

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

9.15.6.6 port-security violation shutdown

このコマンドによりポートセキュリティのバイオレーションシャットダウン属性を有効化します 。

Syntax
port-security violation shutdown no port-security violation shutdown

no -このコマンドによりポートセキュリティのバイオレーションシャットダウン属性を無効化します 。

初期設定

Disabled

コマンド・モード

インターフェイス・コンフィグ

9.15.7 LDAPコマンド

9.15.7.1 show ldap

このコマンドにより現在のLDAP設定を表示します。

Syntax
show ldap

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Server IP: LDAPサーバIP。デフォルト値は 0.0.0.0

Server Port: LDAPサーバのTCPポート。デフォルト値は 389

baseDN: ベース識別名。デフォルト値は空文字列

racName: バインドDNのRDN属性。デフォルト値は空文字列

racDomain: RDNを除いた部分バインドDN。デフォルト値は空文字列

9.15.7.2 ldap ip

このコマンドによりLDAPサーバIPを設定します。

Syntax
ldap ip <ipaddr> no ldap ip

<ipaddr> - IPアドレス 。

no - このコマンドによりIPアドレスをデフォルト値に戻します。

初期設定

0.0.0.0

コマンド・モード

グローバル･コンフィグ

9.15.7.3 ldap port

このコマンドによりLDAPサーバポートを設定します。

Syntax

```
ldap port <portid>
no ldap port
```

<portid> - 1-65535

no - このコマンドによりLDAPサーバポートをデフォルト値に戻します。

初期設定

389

コマンド･モード

グローバル･コンフィグ

9.15.7.4 ldap baseDN

このコマンドによりbaseDNを設定します。

Syntax

```
ldap baseDN <baseDN>
no ldap baseDN
```

<baseDN> -文字列

no - このコマンドによりbaseDNをデフォルト値に戻します。

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.15.7.5 ldap racName

このコマンドによりracNameを設定します。

Syntax
ldap racName <racName> no ldap racName

<racName> - 文字列 。

no - このコマンドによりracNameをデフォルト値に戻します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.15.7.6 ldap racDomain

このコマンドによりracDomainを設定します。

Syntax
ldap racDomain <racDomain> no ldap racDomain

<racDomain> - string.

no - このコマンドによりracDomainをデフォルト値に戻します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.16 差別化サービスコマンド

本章では、QOS差別化サービス(DiffServ)パッケージに使用するCLIコマンドについて説明します。

以下を指定し、複数段階でDiffServを設定します。

4. **クラス**
    - **クラスを作成、削除する**
    - **クラスの一致基準を定義する**

注：既存クラス定義から個別に一致基準を削除するには、そのクラスを削除し、再度作成します。

5. **ポリシー**
    - **ポリシーを作成、削除する**
    - **クラスにポリシーを関連付ける**
    - **ポリシー／クラスの組み合わせのポリシー記述を定義する**
6. **サービス**
    - **方向インターフェイス(インバウンドおよびアウドバウンド)へ(から)、ポリシーを追加または削除する**

パケットは、定義した基準によってフィルタ、処理されます。フィルタ基準はクラスにより、またその処理はポリシー属性により定義されます。ポリシー属性はクラスインターフェイスごとに定義され、基準が一致した場合に適用される属性となります。

パケット処理は、パケットの一致基準のテストで開始します。ポリシーは、ポリシー内でクラスが一致した場合にパケットに適用されます。

注記：all、any、aclのクラスタイプは、クラスを定義した際に指定される一致基準の妥当性に関係します。「any」のクラスタイプは順列シーケンスの一致基準を処理し、このクラスに指定した追加規則がリストに追加されます。「acl」のクラスタイプは、Diffservクラスが作成された際に各ACL規則定義を取り込み、規則リストを取得します。クラスタイプ「all」の一致基準を指定すると、除外しない一致基準フィールドの値が 1 つクラス定義で許可されるため、差異が発生します。フィールドがすでにクラスに指定されている場合、同じフィールドを指定するすべての後続試行が失敗となります。これには、別の形式による複数の方法でフィールドを指定する場合も含まれます。ただし、「exclude」オプションを指定した場合はこの制限が除外フィールドに適用されないため、これには含まれません。

クラス制限について：

- **ネスト化クラスは以下のように制限されます。**
- **「all」内は「all」**
- **条件が「not」の場合、ネスト化されない**
- **クラスタイプが「acl」の場合、ネスト化されない**
- **各クラスで 1 つの参照済みクラスをもつ**

- 階層サービスポリシーはクラス定義で対応しない
- 一致したアクセスリストは参照のみ。クラスの基準となる
- ACL規則は、クラス作成時にクラス一致基準としてコピーされる。クラスタイプは「any」
- 暗黙のACL規則「deny all」もコピーされる
- 「acl」のクラスタイプはネスト化されない

ネスト化クラスはクラス参照といい、別のクラスへの参照 1 つを特定のクラス定義に与え、それを他の一致基準と組み合わせることができます。参照済みクラスに追加を行うと、そのクラス定義を参照するすべてのクラスに影響を与えるため、参照済みクラスは参照でありコピーではありません。他のクラスから現在参照されているクラス定義への変更を行うと、すべての該当クラスの有効クラス定義となり、それ以外の場合、変更は拒否されます。クラス参照は、クラス定義から削除することができます。

クラス、ポリシー、サービスの概要および詳細情報を表示することができます。すべての設定情報はCLI、Web、SNMPのユーザインターフェイスからアクセスできます。

9.16.1 一般コマンド

プラットフォームの以下の項目を設定することができます。

9.16.1.1 diffserv

このコマンドによりDiffServ動作モードをアクティブに設定します。無効の場合、DiffServ設定を保持、変更することができますが、アクティブにすることはできません。有効の場合、DiffServサービスがアクティブとなります。

Syntax
diffserv

コマンド・モード

グローバル・コンフィグ

9.16.1.2 **Classコマンド**

このコマンドによりDiffServ動作モードを非アクティブに設定します。無効の場合、DiffServ設定を保持、変更することができますが、アクティブにすることはできません。有効の場合、DiffServサービスがアクティブとなります。

Syntax
no diffserv

コマンド・モード

グローバル・コンフィグ

9.16.2 クラスコマンド

DiffServの「class」コマンドセットで以下を定義します。

- Traffic Classificationで、DSCPに基づくBehavior Aggregate (BA)、およびトラフィックのMulti- Field (MF) クラス (name、match criteria) を指定します。
- Service Levelsで、BA転送クラス／サービスレベルを指定します。理論上、DiffServは 1. Service/PHB、2. Traffic Classの 2 階層です。

このコマンドセットで、クラスの作成／削除、およびレイヤー3·レイヤー2·標準一致基準を指定するクラス一致コマンドによる一致を行います。クラス一致基準はクラス規則ともいい、1 つまたは複数の規則からなるクラスでトライフック識別を定義しています。クラスが一度作成されると、クラス全体を削除または再度作成する必要があります 。

CLIコマンドルートはclass-mapです。

9.16.2.1 **class-map**

このコマンドによりtype match-all (全タイプに一致) 、match-any (いずれかに一致) 、match-access-group (アクセスグループに一致) の新規DiffServクラスを定義します。

Syntax
class-map [match-all] <class-map-name>

<class-map-name> はクラスを固有に識別する、大文字と小文字で区別される 1～31 文字の英数字です。

注 :クラス名「default」はリザーブされ、ここで使用することはできません。

一致基準を使用しない場合、このコマンドでクラスマップモードが入力されます。

<class-map-name>は既存のDiffServクラス名です。

注 :クラス名「default」はリザーブされ、ここでは許可されません。クラスタイプmatch-allは、すべての一致基準が、クラスのメンバーと判断されるパケットに対しtrueであるる必要があることを示します。クラスタイプmatch-access-groupは、各クラス一致基準がアクセスリスト(ACL)に基づき評価されることを示します。

<aclid>は、既存のACL番号を指定する整数です (有効なACL番号の範囲については、ACLのドキュメンテーションを参照) 。matchaccess-groupのクラスタイプは、指定されたACL番号の現在の規則定義から、一致基準のセットをコピーします。単一のACL規則のすべてのエレメントはallのクラスタイプと同様、DiffServでグループ化セットと判断されます。anyのクラスについては、最低 1 つのクラス一致基準を、有効と判断されるクラスに指定する必要があります。

注 :クラス一致基準は参照済みアクセスリストat the time of class creationから取得されます。そのため、その後参照済みACL定義へ変更を行っても、DiffServクラスには影響を与えません。最新のACL定義を選択するには、DiffServクラスを削除、再度作成する必要があります。このコマンドは、既存のDiffServクラスにClass-Mapコンフィグモードを入力するためのクラスタイプを指定せずに使用することができます。

注 :CLIモードは、コマンドが成功するとClass-Mapコンフィグモードに変更されます。

コマンド・モード

グローバル・コンフィグ

9.16.2.2 **no class-map**

このコマンドにより既存のDiffServクラスを削除します。

Syntax
no class-map <class-map-name>

<class-map-name> は既存のDiffServクラス名です。

注: クラス名「default」はリザーブされ、ここでは許可されません。もし、他のポリシーで使用されている場合、削除することができない場合があります .

コマンド・モード

グローバル・コンフィグ

9.16.2.3 class-map rename

このコマンドによりDiffServクラス名を変更します。

Syntax
class-map rename <class-map-name> <new-class-map-name>

<class-map-name> は既存のDiffServクラス名です。

<new-class-map-name>は、クラスを固有に識別する、大文字と小文字で区別される 1～31 文字の英数字による文字列です。

注: クラス名「default」はリザーブされ、ここで使用することはできません。

デフォルト

なし

コマンド・モード

グローバル・コンフィグ

9.16.2.4 match any

このコマンドによりすべてのパケットがそのクラスに属すると判断する一致基準を、特定のクラス定義に追加します。

Syntax
match any

デフォルト

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.5 match class-map

このコマンドにより他のクラスに定義された一致基準のセットを、特定のクラス定義に追加します。

Syntax
match class-map <refclassname>

<refclassname> は、一致基準が特定のクラス定義で参照される、既存のDiffServクラス名です。

注: この一致コマンドに[not]オプションはありません。

デフォルト

なし

コマンド・モード

Class-Mapコンフィグ

制限： <classname>と<refclassname>のクラスタイプは同じである必要があります（つまりanyとany、またはallとall）。クラスタイプaclはこのコマンドで対応していません。<classname>と同じ名前の<refclassname>を指定することはできません（つまりクラス名の自己参照は許可されません）。1 クラスで他のクラスを 1 つ参照することができます。<classname>から参照されている間、<refclassname>クラスの削除は失敗となります。

<classname>と<refclassname>を組み合わせた一致基準は、クラスタイプに基づき許可された組み合わせである必要があります。<refclassname>のクラス一致基準を後で変更する場合は、妥当性を維持する必要があり、そうでない場合変更は失敗となります。完全な参照クラスチェーン（predecessorクラスとsuccessorクラスの両方を含む）で作成されたクラス規則の合計数は、プラットフォーム指定の最大数を超えてはいけません。refclass規則の削除ごとに、クラス定義内の使用可能規則の最大数が 1 つずつ削除される場合もあります。

9.16.2.6 no match class-map

このコマンドにより他のクラスに定義された一致基準のセットを、特定のクラス定義から削除します。

Syntax
no match class-map <refclassname>

<refclassname> は、一致基準が特定のクラス定義で参照される、既存のDiffServクラス名です。

注: この一致コマンドに[not]オプションはありません。

デフォルト

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.7 match dstip

このコマンドによりパケットの宛先IPアドレスに基づく一致基準を、特定のクラス定義に追加します。

Syntax
match dstip <ipaddr> <ipmask>

<ipaddr>　IPアドレス

<ipmask>　IPアドレスのビットマスク。注記：標準サブネットマスクと似ていますが、このビットマスクは連続させる必要はありません。

デフォルト

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.8 match dstl4port

このコマンドによりキーワードや数値、あるいは数値範囲を使用したパケットの宛先レイヤー4 ポートに基づく一致基準を、特定のクラス定義に追加します。

Syntax
match dstl4port {<portkey> | <0-65535>}

一致基準をキーワードとして指定するには、<portkey>の値に対応ポート名キーワードのうちの 1 つを使用します。現在対応している<portkey>の値はdomain、echo、ftp、ftpdata、http、smtp、snmp、telnet、tftp、wwwです。このそれぞれが同じポート番号に変換され、ポート範囲の開始および終了として使用されます。

数値で一致基準を指定するには、1 つのレイヤー4 ポート番号が必要となります。

ポート番号は 0～65535 の整数です。

数値範囲で一致基準を指定するには、2 つのレイヤー4 ポート番号で、連続するポート範囲を指定する必要があります。各ポート番号は 0～65535 の整数で、2 つめの数は 1 つめの数と同じかそれ以上である必要があります。

デフォルト

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.9 match ip dscp

このコマンドによりIPヘッダのService Typeオクテットの高位 6 ビット (低位 2 ビットはチェックされません) として定義された、パケット内のIP DiffServ Code Point (DSCP) フィールドの値に基づく一致基準を、特定のクラス定義に追加します。

Syntax
match ip dscp <value>

<dscpval>の値は、0～63 の整数のいずれか、またはキーワードaf11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、be、cs0、cs1、cs2、cs3、cs4、cs5、cs6、cs7、efのいずれかで指定されます。

注: ip dscp、ip precedence、ip tos**の一致基準は、IPヘッダにある同じService Typeフィールドの一致基準を指定するための代替方法ですが、ユーザ表記はやや異なります。**

注: すべてのDSCP値に一致基準を指定するには、<tosbits>を 0、<tosmask>を 03 (16 進数) に設定したmatch [not] ip tos <tosbits> <tosmask>**コマンドを使用します。**

デフォルト

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.10 match ip precedence

このコマンドによりIPヘッダのService Typeオクテットの高位 3 ビット (低位 5 ビットはチェックされません) として定義された、パケット内のIP Precedenceフィールドの値に基づく一致基準を、特定のクラス定義に追加します。

Syntax
match ip precedence <0-7>

注: Ip dscp、ip precedence、ip tosの一致基準は、IPヘッダにある同じService Typeフィールドの一致基準を指定するための代替方法ですが、ユーザ表記はやや異なります。.

注: すべてのPrecedenceの値に一致基準を指定するには、<tosbits>を 0、<tosmask>を 1F (16 進数) に設定したmatch [not] ip tos <tosbits> <tosmask>コマンドを使用します。

デフォルト

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.11 match ip tos

このコマンドによりIPヘッダの全 8 ビットのService Typeオクテットとして定義された、パケット内のIP TOSフィールドの値に基づく一致基準を、特定のクラス定義に追加します。

Syntax
match ip tos <tosbits> <tosmask>

<tosbits>は 00 からffまでの 2 桁の 16 進数です。

<tosmask> は 00 からffまでの 2 桁の 16 進数です。

<tosmask>は、パケット内のIP TOSフィールドとの比較に使用する、<tosbits>内のビット位置を示します。例えば、ビット 7 が最大である場合にビット 7 と 5 が設定されビット 1 がクリアされているIP TOSの値を確認するには、<tosbits>にa0 (16 進数) 、<tosmask>にa2 (16 進数) を使用します。

注: Ip dscp、ip precedence、ip tosの一致基準は、IPヘッダにある同じService Typeフィールドの一致基準を指定するための代替方法ですが、ユーザ表記はやや異なります。.

注: これはIP DSCP/Precedence/TOS一致基準の「フリーフォーム」バージョンであり、IP Service Typeフィールドのどのビットをチェックするかをユーザが指定することができます。

デフォルト

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.12 match protocol

このコマンドによりキーワードまたは数値を使用したパケットのIP Protocolの値に基づく一致基準を、特定のクラス定義に追加します。

Syntax
match protocol {<protocol-name> | <0-255>}

<protocol-name> は、対応プロトコル名キーワードの 1 つです。現在対応している値はicmp、igmp、ip、tcp、udpです。注記：ipの値は、すべてのプロトコル番号に一致すると判断されます。数値を使用した一致基準を指定するには、プロトコル番号をIANAに割り当てられた標準値にし、0～255 の整数として判断される必要があります。

注: このコマンドによりIANAに定義された現在のリストに対しプロトコル番号の値は検証しません。

デフォルト

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.13 match srcip

このコマンドによりパケットの送信元IPアドレスに基づく一致基準を、特定のクラス定義に追加します 。

Syntax
match srcip <ipaddr> <ipmask>

<ipaddr> IPアドレス。

<ipmask> IPアドレスビットマスクを指定します。注記：標準サブネットマスクと似ていますが、このビットマスクは連続させる必要はありません。

デフォルト

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.14 match srcl4port

このコマンドによりキーワードや数値、あるいは数値範囲を使用したパケットのソースレイヤー4 ポートに基づく一致基準を、特定のクラス定義に追加します。

Syntax
match srcl4port {<portkey> | <0-65535>}

<portkey> は、対応するポート名キーワードの 1 つです (下記リスト参照) 。

現在対応している<portkey>の値はdomain、echo、ftp、ftpdata、http、smtp、snmp、telnet、tftp、wwwです。

数値で一致基準を指定するには、1 つのレイヤー4 ポート番号が必要となります。ポート番号は 0～65535 の整数です。

数値範囲で一致基準を指定するには、2 つのレイヤー4 ポート番号で、連続するポート範囲を指定する必要があります。各ポート番号は 0～65535 の整数で、2 つめの数は 1 つめの数と同じかそれ以上である必要があります。

デフォルト

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.15 match cos

このコマンドによりサービス値のクラス (単一タグ済みパケットのタグ、または二重VLANタグ済みパケットの第一タグあるいは外部 802.1Qタグ) の一致基準を、特定のクラス定義に追加します。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match cos <0-7>

初期設定

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.16 match destination-address mac

このコマンドによりパケットの宛先MACアドレスに基づく一致基準を、特定のクラス定義に追加します。<address>パラメータは、コロンで分割された 2 桁の 16 進数 6 組 (例：00:11:22:dd:ee:ff) の形式のレイヤー2 MACアドレスです。<mac-mask>パラメータは、コロンで分割された 2 桁の 16 進数 6 組 (例：ff:07:23:ff:fe:dc) の形式のレイヤー2 MACアドレスビットマスクで、連続する必要はありません。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match destination-address mac <address> <mac-mask>

<address> - レイヤー2 MACアドレスを指定します

<mac-mask> - レイヤー2 MACアドレスビットマスクを指定します。

初期設定

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.17 match ethertype

このコマンドによりethertypeの値に基づく一致基準を、特定のクラス定義に追加します。<ethertype>の値はappletalk、arp、ibmsna、ipv4、ipv6、ipx、mplsmcast、mplsucast、netbios、novell、pppoe、rarpのキーワード、または0x0600～0xFFFFの範囲のカスタムethertype値で指定します。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match ethertype {<keyword> | <0x0600-0xFFFF>}

<keyword> - appletalk、arp、ibmsna、ipv4、ipv6、ipx、mplsmcastなどを指定します。

<0x0600-0xFFFF> - ethertype値を指定します。

初期設定

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.18 match secondary-cos

このコマンドによりサービス値のセカンダリクラス (二重VLANタグ済みパケットの内部 802.1Qタグ) の一致基準を、特定のクラス定義に追加します。の一致基準を、特定のクラス定義に追加します。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match secondary-cos <0-7>

初期設定

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.19 match secondary-vlan

このコマンドによりレイヤー2 セカンダリVLAN識別子フィールドの値 (二重VLANタグ済みパケットの内部 802.1Qタグ) に基づく一致基準を、特定のクラス定義に追加します。セカンダリVLAN IDは、0～4095 の整数です。

注:このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match secondary-vlan <0-4095>

初期設定

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.20 match source-address mac

このコマンドによりパケットの送信元MACアドレスに基づく一致基準を、特定のクラス定義に追加します。<address> パラメータは、コロンで分割された 2 桁の 16 進数 6 組 (例: 00:11:22:dd:ee:ff) の形式のレイヤー2 MACアドレスです。<mac-mask>パラメータは、コロンで分割された 2 桁の 16 進数 6 組 (例: ff:07:23:ff:fe:dc) の形式のレイヤー2 MAC アドレスビットマスクで、連続する必要はありません 。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match source-address mac <address> <macmask>

<address> - レイヤー2 MACアドレスを指定します。

<macmask> - レイヤー2 MACアドレスビットマスクを指定します。

初期設定

なし

コマンド・モード

Class-Mapコンフィグ

9.16.2.21 **match vlan**

このコマンドによりレイヤー2 VLAN識別子フィールドの値 (単一タグ済みパケットのタグ、またはVLANタグ済みパケットの第一タグまたは外部タグ) に基づく一致基準を、特定のクラス定義に追加します。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match vlan <0-4095>

初期設定

なし

コマンド・モード

Class-Mapコンフィグ

9.16.3 Policyコマンド

DiffServの「policy」コマンドセットで、以下を定義します。

Traffic Conditioningで、トラフィッククラスに適用するトラフィック条件動作（ポリシング、marking、shaping）を指定します。

Service Provisioningで、サービスレベル（EF、AFなど）の帯域およびキュー深度管理要件を指定します。

ポリシーコマンドを使用し、クラスコマンドセットで定義されたトラフィッククラスと、1 つまたは複数のQoSポリシー属性を関連付けます。関連付けは、サービスを作成するため特定方向のインターフェイスに割り当てられます。ポリシーが作成されたらポリシー名を指定します。

DiffServ CLIで、ユーザが１つのトラフィッククラスを１つのポリシーに 関連付ける必要がある わけではあ りま せん。実際、複数のトラフィッククラスを 1 つのポリシーに関連付け、クラス定義に一致するパケットの特定処理を定義することができます。パケットが複数クラスの条件を満たした場合、クラスがポリシーに追加された順番に基づきプライオリティが決定するため、一番前にあるクラスが最優先されます。

このコマンドセットは、ポリシー作成／削除、クラス追加／削除、ポリシー属性で構成されています。注記：ポリシー内のクラスインスタンスからポリシー属性を削除するには、クラスインスタンスを削除してから再度ポリシーに追加します。既存のポリシー属性に関連付いている値は、クラスインスタンスを削除せずに変更することができます。

CLIコマンドルートはpolicy-mapです。

9.16.3.1 assign-queue

このコマンドにより関連トラフィックストリームが割り当てられているキューIDを修正します。queueidは 0〜n-1 の整数で、nはデバイスが対応している送信キューの数です。

Syntax
assign-queue <0-7>

<0-7> - キューID。

(*)<0-6> - キューID。

*注: (*はスタッキングコマンドです。*

コマンド・モード

Policy-Class-Mapコンフィグ

9.16.3.2 **drop**

このコマンドにより関連トラフィックストリームのすべてのパケットを受信時にドロップするよう指定します。

Syntax
drop

コマンド・モード

Policy-Class-Mapコンフィグ

9.16.3.3 **mirror**

このコマンドにより関連トラフィックストリームのすべての受信パケットを、特定の送信インターフェイス (物理ポートまたはLAG) にコピーするよう指定します。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
mirror <slot/port>

<slot/port> - インターフェイス番号。

初期設定

なし

コマンド・モード

Policy-Class-Mapコンフィグ

9.16.3.4 redirect

このコマンドにより関連トラフィックストリームのすべての受信パケットを、特定の送信インターフェイス (物理ポートまたはポートチャネル) にリダイレクトするよう指定します。

Syntax
redirect <slot/port>

コマンド・モード

Policy-Class-Mapコンフィグ

9.16.3.5 conform-color

このコマンドによりカラー認識トラフィックポリシングを有効化し、使用されている適合カラークラスマップを定義します。一致レベルのフィールド (simple、single-rate、two-rate policing) が指定されている場合、policeコマンドと共に使用します。<class-map-name>パラメータは、適合カラーおよび超過カラーで異なる名前を使用する必要がある場合、既存のDiffservクラスマップ名となります。

Syntax
conform-color <class-map-name>

<class-map-name> -適合カラーに異なる名前を使用する必要がある場合の、既存のDiffservクラスマップ名。

コマンド・モード

Policy-Class-Mapコンフィグ

9.16.3.6 **mark cos**

このコマンドにより 802.1pヘッダーの優先フィールド内にある、サービス値の特定クラスと関連付けられたトラフィックストリームの、すべてのパケットをマークします。パケットがこのヘッダーにない場合、1 が挿入されます。CoSの値は 0～7 の整数です。

Syntax
mark cos <0-7>

<0-7> - CoS値の範囲は 0～7。

コマンド・モード

Policy-Class-Mapコンフィグ

Policy Type In//ポリシー・タイプ In

9.16.3.7 mark ip-dscp

このコマンドにより特定のIP DSCP値と関連付けられたトラフィックストリームの、すべてのパケットをマークします。

Syntax
mark ip-dscp <value>

<value>は、0～63 の整数のいずれか、またはキーワードaf11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、be、cs0、cs1、cs2、cs3、cs4、cs5、cs6、cs7、efのいずれかで指定されます。

コマンド・モード

Policy-Class-Mapコンフィグ

Policy Type In/**ポリシー・タイプ** In

Incompatibilities Mark IP Precedence, Police （全形式）

9.16.3.8 mark ip-precedence

このコマンドにより特定のIP Precedence値と関連付けられたトラフィックストリームの、すべてのパケットをマークします。IP Precedenceの値は 0～7 の整数です。

Syntax
mark ip-precedence <0-7>

コマンド・モード

Policy-Class-Mapコンフィグ

Policy Type In/**ポリシー・タイプ** In

Incompatibilities Mark IP DSCP, Police （全形式）

9.16.3.9 police-simple

このコマンドにより特定クラスのトラフィックポリシングスタイルを確立します。

Syntax
police-simple {<1-4294967295> <1-128> conform-action {drop | set-cos-transmit <0-7> | set-prec-transmit <0-7> | set-dscp-transmit <value> | transmit} [violate-action {drop | set-prectransmit <0-7> | set-dscp-transmit <0-63> | transmit}]}

policeコマンドでは単一のデータレートとバーストサイズの形式を使用し、以下 2 通りの結果となります。

<conform-action & violate-action>：一致データレートがキロビット／秒 (Kbps) 単位で指定され、1～4294967295 の整数となります。一致バーストサイズはキロバイト (KB) 単位で指定され、1～128 の整数となります。結果で実施される動作はdrop、set-dscp-transmit、set-prec-transmit、transmitです。policeコマンドの形式で、一致動作がtransmitに戻り、バイオレーション動作がdropに戻ります。動作はスタイルを設定するとこのコマンドで設定することができます。<set-cos-transmit>で、プライオリティの値が要求され、0～7 の整数で指定されます。<set-dscp-transmit>が要求され、0～63 の整数のいずれか、またはキーワードaf11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、be、cs0、cs1、cs2、cs3、cs4、cs5、cs6、cs7、efのいずれかで指定されます 。

<set-prec-transmit>で、IP Precedenceの値が要求され、0～7 の整数で指定されます。

コマンド・モード

Policy-Class-Mapコンフィグ

Restrictions:policeコマンドのsimpleのみが特定ポリシーのクラスインスタントに許可されます。

Policy Type In

Incompatibilities Mark COS, Mark IP DSCP, Mark IP Precedence

9.16.3.10 class

このコマンドにより後続ポリシー属性記述を使用しトラフィッククラスの処理を定義するため、特定ポリシー内にクラス定義のインスタンスを作成します。

Syntax
class <classname>

<classname> は既存のDiffServクラス名です。注記：このコマンドにより特定ポリシーがクラス定義への参照を作成します。

コマンド・モード

Policy-Class-Mapコンフィグ

9.16.3.11 no class

このコマンドにより特定クラスのインスタンスおよび定義済み処理を、特定ポリシーから削除します。

Syntax
no class <classname>

<classname> は既存のDiffServクラス名です。注記：このコマンドにより特定ポリシーのクラス定義への参照を削除します。

コマンド・モード

Policy-Class-Mapコンフィグ

9.16.3.12 policy-map

このコマンドにより新規のDiffServポリシーを確立します。<policyname>パラメータはポリシーを固有に識別するための、大文字と小文字で区別される 1～31 文字の英数字です。ポリシーのタイプはパラメータに示されているインバウンドトラフィックの方向となります。

Syntax
policy-map <policyname> [in] no policy-map <policyname>

コマンド・モード

グローバル・コンフィグ

Policy Type In//ポリシー・タイプ In

9.16.3.13 policy-map rename

このコマンドによりDiffServポリシー名を変更します。<policyname>は既存のDiffServクラス名です。<newpolicyname>パラメータはポリシーを固有に識別するための、大文字と小文字で区別される1～31文字の英数字です。

Syntax
policy-map rename <policyname> <newpolicyname>

<policyname> -旧ポリシー名。

<newpolicyname> -新規ポリシー名。

コマンド･モード

グローバル･コンフィグ

Policy Type In//**ポリシー･タイプ** In

9.16.4 Serviceコマンド

DiffServの「service」コマンドセットで、以下を定義します。

Traffic Conditioning：DiffServトラフィック条件ポリシー（ポリシーコマンドで指定）を、受信方向のイン ターフェイスに割り当てます。

Service Provisioning：DiffServサービス提供ポリシー（ポリシーコマンドで指定）を、送信方向のイン ターフェイスに割り当てます。

サービスコマンドで、方向インターフェイスに定義済みポリシーを付与します。1 ポリシーのみを、特定方向のインターフェイスにいつでも割り当てることができます。ポリシータイプ（in、out）は、付与するインターフェイスの方向と一致する必要があります。

このコマンドセットでサービスの追加／削除を行います。

CLIコマンドルートはservice-policyです。

9.16.4.1 service-policy

このコマンドにより特定方向のインターフェイスにポリシーを付与します。

Syntax
service-policy in <policy-map-name>

このコマンドをInterface Configモードで使用し、ポリシーを特定のインターフェイスに付与することが できます。 あるいは、このコマンドをGlobal Configモードで使用し、すべてのシステムインターフェ イスにポリシーを付 与することもできます。 方向の値はinまたはoutです。

<policy-map-name>は既存のDiffServポリシー名であり、タイプがインターフェイスの方向 と一致する必要 があ ります。注記：このコマンドによりサービスによりポリシーに参照が作成されます。

注: このコマンドによりインターフェイス上のDiffServを有 効化します（特定方向）。 その他のDiffServ用イ ンターフ ェイス 管理の「mode」コマンドはありません。

注: このコマンドは、ポリシー定義内の属性がインターフェイスの上限を超え ると失敗と なります。 ポリシーがインターフェイスに正しく付与されると、インターフェイス上限違反とするポリシー定義を変更してもそのポリシー変更は失敗となります。

コマンド・モード

グローバル・コンフィグ（すべてのシステムインターフェイス用）

インターフェイス・コンフィグ（特定のインターフェイス用）

Restrictions 1 ポリシーのみを、特定方向のインターフェイスにいつでも付与することができます。

9.16.4.2 **no service-policy**

このコマンドにより特定方向のインターフェイスからポリシーを削除します。

Syntax
no service-policy in <policy-map-name>

このコマンドをInterface Configモードで使用し、ポリシーを特定のインターフェイスから削除すること ができます。あるいは、このコマンドをGlobal Configモードで使用し、現在ポリシーが付与されているすべてのシステム インターフェイスからポリシーを削除することもできます。方向の値はinまたはoutです。

<policy-map-name> は、既存のDiffServポリシー名です。注記：このコマンドによりサービ スによりポリシ ーへ の参照が削除されます。

注: このコマンドによりインターフェイス上のDiffServを無効化します (特定方向) 。

その他のDiffServ用インターフェイス管理の「mode」コマンドはありません。

コマンド・モード

グローバル・コンフィグ (すべてのシステムインターフェイス用)

インターフェイス・コンフィグ (特定のインターフェイス用)

9.16.5 Showコマンド

DiffServで「show」コマンドセットを使用し、以下の設定とステータス情報を表示します。

- クラス
- ポリシー
- サービス

この情報は、概要または詳細形式で表示することができます。ステータス情報は、DiffServ管理モードが有効の場合にのみ表示され、それ以外の場合は表示されません。また、「show」コマンドでDiffServの一般情報をいつでも表示することができます。

9.16.5.1 show diffserv

このコマンドによりメインDiffServプライベートMIBテーブルの現在数および最大数の列や現在の管理モード設定などの、DiffServ一般ステータスグループ情報を表示します。

Syntax
show diffserv

初期設定

なし

コマンド・モード

特権EXECおよびユーザ EXEC

表示メッセージ

DiffServ Admin Mode: DiffServ管理モードの現在の値

Class Table Size Current/Max: クラステーブルのエントリ（列）の現在数または最大数

Class Rule Table Size Current/Max: クラス規則テーブルのエントリ（列）の現在数または最大数

Policy Table Size Current/Max: ポリシーテーブルのエントリ（列）の現在数または最大数

Policy Instance Table Size Current/Max: ポリシーインスタンステーブルのエントリ（列）の現在数または最大数

Policy Attribute Table Size Current/Max: ポリシー属性テーブルのエントリ（列）の現在数または最大数

Service Table Size Current/Max: サービステーブルのエントリ（列）の現在数または最大数

9.16.5.2 show diffserv service

このコマンドにより特定のインターフェイスおよび方向のポリシーサービス情報を表示します。

Syntax
show diffserv service <slot/port> in

<slot/port>で、システムの有効スロット番号およびポート番号を指定します。directionパラメータは、インターフェイスの対象方向を示します。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

DiffServ Admin Mode: DiffServ管理モードの現在の設定。付与されたポリシーは、DiffServのモー ドが有 効の 場合にインターフェイス上で有効化されます。

Interface: インターフェイスのスロット番号およびポート番号 (スロット／ポート)

Direction: このインターフェイスサービスのトラフィック方向

Operational Status: DiffServサービスインターフェイスの現在の動作ステータス

Policy Name: 表示方向のインターフェイスに付与されたポリシー名

Policy Details: 付与されたポリシー詳細。内容はshowポリシーマップの<policymapname>コマン ドと同じで す(ここでの内容説明は省略します)。

9.16.5.3 show diffserv service brief

このコマンドによりDiffServポリシーが付与された、システム上のすべてのインターフェイスを表示します。direction パラメータは任意です。指定されている場合、その方向のサービスのみが表示されます。

Syntax
show diffserv service brief [in]

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

DiffServ Admin Mode: DiffServ管理モードの現在の設定。付与されたポリシーは、 DiffServ の モードが 有効の間、インターフェイス上のみでアクティブとなります。

以下の情報はインターフェイスおよび方向について繰り返されます（付与されたポリシーで設定されたインターフェイスのみが表示されます）：

Interface: インターフェイスのスロット番号およびポート番号（スロット／ポート）

Direction: このインターフェイスサービスのトラフィック方向

Operational Status: DiffServサービスインターフェイスの現在の動作ステータス

Policy Name: 表示方向のインターフェイスに付与されたポリシー名

9.16.5.4 **show class-map**

このコマンドにより特定クラスのすべての設定情報を表示します。

Syntax
show class-map [<classname>]

<classname> は既存のDiffServクラス名です。

初期設定

なし

コマンド・モード

特権EXECおよびユーザ EXEC

表示メッセージ

Class Name: クラス名

Class Type:このクラスに対し一致基準が評価される方法を示すクラスタイプ (all、any、acl) 。 クラス タイプallは、このクラスに定義された一致基準が同時に評価され、すべてtrueの場合にクラスが一致していることを示します。タイプanyは、一致基準が順番に評価され、いずれか 1 つがtrueの場合にクラスが一致していることを示します。タイプaclは複合方法で評価するもので、各ACL規則によってグループ化と評価が同時に行われたものが順番に評価されます。

Match Criteria: Match Criteriaフィールドは、設定されているかどうかのみを示すもので、ユーザが入力 した順番で内容が表示されます。クラスタイプに基づき評価が行われます。Match Criteriaフィールドの値は、Class of Service、Destination IP Address、Destination Layer 4 Port、Destination MAC Address、Every、IP DSCP、IP Precedence、IP TOS、Protocol Keyword、Reference Class、Source IP Address、Source Layer 4 Port、Source MAC Address、VLANです。

Values: Match Criteriaの値を示します。

Excluded: Match Criteriaが除外されているかを示します。クラス名が指定されていない場合、 このコ マンドですべての定義済みDiffServクラスの一覧を表示します。表示されるフィールドは以下のとおりです

Class Name: クラス名

Class Type:このクラスに対し一致基準が評価される方法を示すクラスタイプ (all、any、acl) 。クラスタイプallは、このクラスに定義された一致基準が同時に評価され、すべてtrueの場合にクラスが一致していることを示します。タイプanyは、一致基準が順番に評価され、いずれか 1 つがtrueの場合にクラスが一致していることを示します。タイプaclは複合方法で評価するもので、各ACL規則によってグループ化と評価が同時に行われたものが順番に評価されます。

ACL Number: クラス作成時にクラス一致基準を定義するためのACL番号。クラスタイプaclの場合のみこのフィールドを使用します (注記：ACLの内容は、クラス作成後変更されている場合があります) 。

Ref Class Name: 特定のクラス定義で参照された一致基準である、既存のDiffServクラス名。

9.16.5.5 **show policy-map**

このコマンドにより特定ポリシーのすべての設定情報を表示します。

Syntax
show policy-map [<policy-map-name>]

<policy-map-name> は既存のDiffServポリシー名です。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Policy Name: ポリシー名

Policy Type: ポリシー定義がインバウンドであるかアウトバウンドであるかを示します。

以下の情報はこのポリシーに関連する各クラスについて繰り返されます:

(実際に設定されたポリシー属性のみが表示されます):

Class Name: クラス名。

Mark CoS: アウトバウンドパケットの 802.1pヘッダーで設定されたサービス値のクラスを示します。mark cosを指定していない場合は表示されません。

Mark IP DSCP: このクラスに一致するトラフィックのDSCPとして使用されるmark/re-markの値を示します。police-two-rateコマンドを使用してmark ipの記述が指定されていない場合、またはこのポリシーに従ったクラスにポリシングが使用されている場合は表示されません。

Mark IP Precedence: このクラスに一致するトラフィックのIP Precedenceとして使用されるmark/re-markの値を示します。このポリシーに従ったクラスに、mark DSCPまたはポリシングが使用されている場合は表示されません。

Policing Style: ポリシングのスタイルがあればsimpleと表示します。

Committed Rate (Kbps): シンプルポリシングのコミットレートをsingle-rate policingおよびtwo-rate policingで表示します。

Committed Burst Size (KB): シンプルポリシングのコミットバーストサイズを示します。

Conform Action: policingパラメータに適合すると判断されたパケットで適用されている現在の設定。このポリシーに従ったクラスでポリシングが使用されていない場合は表示されません。

Conform COS Value: 適合動作がmarkcosである場合、プライオリティマークの値を示します。

Conform DSCP Value: 適合動作がmarkdscpである場合、DSCPマークの値を示します。

Conform IP Precedence Value: 適合動作がmarkprecである場合、IP Precedenceマークの値を示します。

Non-Conform Action: policingパラメータに適合しない判断されたパケットで適用されている現在の設定。このポリシーに従ったクラスでポリシングが使用されていない場合は表示されません。

Non-Conform DSCP Value: 適合動作がmarkdscpである場合、DSCPマークの値を示します。

Non-Conform IP Precedence Value: 適合動作がmarkprecである場合、IP Precedenceマークの値を示します。

Bandwidth: リザーブされた最低帯域をパーセントまたはキロビット／秒のいずれかで示します。

Policy Name: ポリシー名（注記：ポリシーの表示は作成順ではありません）

Policy Type: ポリシー定義がインバウンドであるかアウトバウンドであるかを示します。

Class Members: このポリシーに関連するすべてのクラス名の一覧を表示します。

9.16.5.6 show policy-map interface

このコマンドにより特定のインターフェイスおよび方向について、ポリシー関連の統計データを表示します。

Syntax
show policy-map interface <slot/port> in

<slot/port> で、システムの有効スロット番号およびポート番号を指定します。directionパラメータは、インターフェイスの対象方向を示します。

コマンド・モード

特権EXEC

表示メッセージ

Interface: インターフェイスのスロット番号およびポート番号（スロット／ポート）

Direction: このインターフェイスサービスのトラフィック方向。inまたはout

Operational Status : DiffServサービスインターフェイスの現在の動作ステータス

Policy Name: 表示方向のインターフェイスに付与されたポリシー名

Interface Offered Octets/Packets: 定義済みのDiffServ処理が適用される前に、特定方向のサービスインターフェイスに与えられたオクテット／パケットの累積数

Interface Discarded Octets/Packets: DiffServ処理のため、特定方向のサービスインターフェイスにより破棄されたオクテット／パケットの累積数

Interface Sent Octets/Packets: 定義済みのDiffServ処理が適用された後に、特定方向のサービスインターフェイスから転送されたオクテット／パケットの累積数。この場合の転送とは、スイッチ機能やルーティング機能、またはアウトバウンドリンク送信エレメントなど、データパス内の次の機能エレメントにトラフィックストリームが送信されたことを示します。

以下の情報はこのポリシー内の各クラスインスタンスについて繰り返されます：

Class Name: クラスインスタンス名

In Offered Octets/Packets: 定義済みのDiffServ処理が適用される前に、このクラスインスタンスに与え られたオクテット／パケットの数。方向が「in」の場合のみ表示されます。

In Discarded Octets/Packets: トラフィッククラスのDiffServ処理のため、このクラスイ ンスタンスで破棄されたオクテット／パケットの数。方向が「in」の場合のみ表示されます。

Tail Dropped Octets/Packets: 送信キューからのテールドロップ、特にトラフィックシェーピン グにより 破棄された、オクテット／パケットの数。プラットフォームによってはこの数に対応していない場合があります。方向が「out」の場合のみ表示されます。

Random Dropped Octets/Packets: WREDアクティブキュー深度管理のトラフィックシェー ピングの ため 破棄された 、オクテット／パケットの数。この数はすべてのプラットフォームで対応している わけで はなく 、ポ リシー属性にランダムドロップが含まれたクラスインスタンスのみに使用されます。方向が「out」の場合のみ表示されます。

Shape Delayed Octets/Packets: トラフィックシェーピングのため遅延したオクテット／パケ ットの数。 この 数はすべてのプラットフォームで対応しているわけではなく、ポリシー属性にランダムドロップが含まれたクラスインスタンスのみに使用されます。方向が「out」の場合のみ表示されます。

Sent Octets/Packets: 定義済みのDiffServ処理が実施された後、このクラスインスタンスに転送された オクテット／パケットの数。この場合の転送とは、スイッチ機能やルーティング機能、またはアウトバウンドリンク送信エレメントなど、データパス内の次の機能エレメントにトラフィックストリームが送信されたことを示します。方向が「out」の場合のみ表示されます。

注: 上記のカウンタはすべてのプラットフォームで対応しているわけではありません。 対応しているカウ ンタのみが表示されます。

9.16.5.7 show service-policy

このコマンドにより特定方向のすべてのインターフェイスのポリシー関連統計データを表示します。Directionパラメータは、インターフェイスの対象方向を示します。このコマンドでルートリフレクタクライアントを有効化または無効化します。ルートリフレクタクライアントは、AS全体にルートを再度アドバタイズするルートリフレクタに従います。値はenableまたは*disable*です。

Syntax
show service-policy [in]

コマンド・モード

特権EXEC

表示メッセージ

以下の情報は各インスタンスおよび方向について繰り返されます（付与されたポリシーに設定されたインターフェイスのみが表示されます）：

Interface: インターフェイスのスロット番号およびポート番号（スロット／ポート）

Operational Status: DiffServサービスインターフェイスの現在の動作ステータス

Policy Name: インターフェイスに付与されたポリシー名

注: 上記のカウンタはすべてのプラットフォームで対応しているわけではありません。 対応しているカウンタのみが表示されます。

9.17 ACLコマンド

9.17.1 Showコマンド

9.17.1.1 show mac access-lists

このコマンドによりMACアドレスリスト、およびACLに定義されたすべての規則を表示します。<name>パラメータで、表示する特定のMAC ACLを識別します。

Syntax
show mac access-list <name>

<name> は表示するMAC ACLを固有に識別するACL名です。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

MAC ACL Name: MAC ACL規則名

Rule Number: ACLで定義された順列規則数の識別子

Action: 規則に関連した動作。値はPermitまたはDeny

Source MAC Address: 規則の送信元MACアドレス

Source MAC Mask: 規則の送信元MACマスク

Destination MAC Address: 規則の宛先MACアドレス

Destination MAC Mask: 規則の宛先MACマスク

Ethertype: 規則のEthertypE-KEYワードまたはカスタム値

VLAN ID: 規則のVLAN識別子の値または範囲

CoS Value: 規則のCOS (802.1p)の値

Secondary VLAN ID: 規則のセカンダリVLAN識別子の値または範囲

Secondary COS: 規則のセカンダリCOS (802.1p)の値

Assign Queue: 規則に一致するパケットが割り当てられているキュー識別子

Redirect Interface: 規則に一致するパケットが転送されるスロット／ポート

9.17.1.2 show mac access-lists

このコマンドによりシステム内のすべての定義済みMACアクセスリストの概要を表示します。

Syntax
show mac access-list

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Current number of all ACLs: ACLに定義されたユーザ設定規則の数

Maximum number of all ACLs: ACL規則の最大数

MAC ACL Name: MAC ACL規則名。

Rules: ACLの規則数

Direction: 列記されたインターフェイスにMAC ACLが付与される方向。値はInboundまたはOutbound

Interface: MAC ACLが特定方向で付与されるインターフェイス (スロット／ポート) のリスト

9.17.1.3 show ip access-lists

このコマンドによりアクセス制御リスト (ACL) 、およびACLに定義されているすべての規則を表示します。

Syntax
show ip access-lists [<1-199>]

<1-199>はACLを識別する数です。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Current number of ACLs: ACLに定義されたユーザ設定規則の数

Maximum number of ACLs: ACL規則の最大数

ACL ID: ACLの識別子

Rule: ACLに定義された規則の番号識別子

Action: これは各規則と関連付けられた動作を表示します。とりうる値はPermitまたはDenyです。

Match ALL Match: すべてのパケットまたはなし

Protocol: 規則をフィルタするプロトコル

Source IP Address: 規則の送信元IPアドレス

Source IP Mask: 規則のソースIPアドレスマスク

Source Ports: 規則のソースポートの範囲

Destination IP Address: 規則の宛先IPアドレス

Destination IP Mask: 規則の宛先IPマスク

Destination Ports: 規則の宛先ポートの範囲

Service Type Field Match: IP DSCP、IP Precedence、IP TOSの一致基準が規則に指定されているかを示します。

Service Type Field Value: Service Type Field Matchに指定されている値（IP DSCP、IP Precedence、IP TOS）

9.17.1.4 show access-lists interface

このコマンドにより方向が「in」の特定インターフェイスのアクセスリスト情報を表示します。

Syntax
show access-lists interface <slot/port> in

<slot/port> はインターフェイス番号です。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

ACL Type: ACLタイプがIPまたはMACであるかを示します。

ACL ID: ACL IDを示します。

Sequence Number: インターフェイスおよび方向に関連付けられている他のアクセスリストに関連す るアク セスリストの順番。順番は番号順です。

9.17.2 Configコマンド

9.17.2.1 mac access-list extended

このコマンドによりEthernetフレームのレイヤー2 ヘッダーに定義された分類フィールドのある、<name>で識別されたMACアクセス制御リスト（ACL）を作成します。<name>パラメータは大文字と小文字で区別される1～31文字の英数字で、MACアドレスリストを固有に識別します。同じ名前のMAC ACLがすでに存在する場合、このコマンドでMac Access-list コンフィグモードを入力し、既存のACLを更新することができます。

Syntax
mac access-list extended <name> no mac access-list extended <name>

<name> - MACアドレスリストを固有に識別します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.17.2.2 mac access-list extended

このコマンドによりMACアクセス制御リスト（ACL）の名前を変更します。<name>パラメータは既存のMAC ACLの名前です。<newname>パラメータは大文字と小文字で区別される 1～31 文字の英数字で、MACアクセスリストを固有に識別します。<newname>のMAC ACL名が存在する場合、このコマンドは失敗となります

Syntax
mac access-list extended rename <name> <newname>

<name> - MACアクセスリストを固有に識別する前回の名前

<newname> - MACアクセスリストを固有に識別する新規の名前

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.17.2.3 mac access-list

このコマンドにより現在のMACアドレスリストに規則を新規作成します。各規則は、アドレスリストの設定規則リストに付与されます。「deny all」のMAC規則で、アクセスリストをつねに終了します。 注記：ACL内の規則を個別に削除することはできないため、「no」のコマンドには対応していません。そのためACL全体を削除し再度指定する必要があります。

特定の分類フィールドに応じて、規則でトラフィックを拒否または許可します。少なくとも、送信元MACと宛先MACの値とマスクペアを指定する必要があり、フィールドのいずれかの値に一致することを示す「any」のキーワードで代替することができます。BPDU MACの値 01-80-c2-xx-xx-xx (16 進数。「xx」は不問) を示す 宛先MAC の値 ／マスクに、「bpdu」のキーワードを指定することができます。残りのコマンドパラメータはすべて任意となります。Ethertypeは、キーワード、または 0x0600～0xFFFFの 4 桁の 16 進数で指定します。現在対応している <ethertypekey>の値はppletalk、arp、ibmsna、ipv4、ipv6、ipx、mplsmcast、mplsucast、netbios、novell、pppoe、rarpです。この値は、同じEthertype値に変換されます。割り当てキューのパラメータにより、特定ハードウェアキューの仕様で、この規則に一致するトラフィックを処理します。許可される<queue-id>の値は 0～(n-1)で、nはハードウェアプラット フォームで使用できるユーザ設定可能キューの数です。redirectパラメータにより、この規則に一致するトラフィックを特定の<slot/port>に転送することができます。割り当てキューおよびredirectパラメータは、permit の規則の みで有効化されます 。

Syntax
{deny | permit} {{<srcmac> <srcmask>} | any} {{<dstmac> <dstmask>} | any | bpdu} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {{eq <0-4095>}} [cos <0-7>] [<secondary-vlan {{eq <0-4095>}} [secondary-cos <0-7>] [log] [assign-queue <queue-id>] [{mirror | redirect} <slot/port>] [<rule-id>]

初期設定

なし

コマンド･モード

Mac Access-list コンフィグ

9.17.2.4 mac access-group in

このコマンドにより特定方向のインターフェイスに、<name>で識別された特定のMACアクセス制御リスト (ACL) を付与します。<name>パラメータは既存のMAC ACLの名前である必要があります。任意のシーケンス番 号で 、こ の インターフェイスと方向に割り当てられている他のアクセスリストに関連する、アクセスリストの順番を指定します。順番は番号順です。シーケンス番号がこのインターフェイスと方向に使用されている場合、シーケンス番号を使用して、現在付与されているアクセスリストが特定のアクセスリストで置き換えられます。シーケンス番号がこのコマンドに指定されていない場合、このインターフェイスと方向で現在使用されている最大シーケンス番号より大きいシーケンス番号が使用されます。「InterfaceConfig」モードで指定したこのコマンドは 1 インターフェイスのみに適用され、 「Global Config」モード設定はすべてのインターフェイスに適用されます。「Interface Config」 モードコ マンドは、サービスキュー設定の独立ポート単位クラスに対応したプラットフォーム上のみで使用することができます。

Syntax
mac access-group <name> in [<1-4294967295>] no mac access-group <name> in

<name> - MACアドレスリストを固有に識別します。

<1-4294967295> - ACLのシーケンス番号 。

no - このコマンドにより特定方向のインターフェイスから、<name>で識別されたMAC ACLを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ、インターフェイス・コンフィグ

9.17.2.5 access-list

このコマンドによりパラメータで識別されたアクセス制御リスト (ACL) を作成します。

Syntax
access-list {(<1-99> {deny | permit} {every | <srcip> <srcm ask>}) | ({<100-199> {deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} any | <srcip> <srcmask> [{eq {<portvalue> | <portkey>}](any | <dstip> <dstmask>) [{eq {<portvalue> | <portkey>}] {[precedence <precedence>] | [tos <tos> <tosmask>] | [dscp <dscp>] [log] [assign-queue <queue-id>] [{mirror | redirect} <slot/port>] [<rule-id>]}}}}})

<accesslistnumber>：ACL番号は 1～199 の整数です。1～99 は通常のACLリスト、100～199 は拡張ACLリストです。

permit or deny：ACL規則は 2 つのオプションで作成されます。 ACL規則をフィルタするプロトコルに、 icmp、igmp、ip、tcp、udpの 使用を指定します。このコマンドによりsrcip and srcmask parametersで指定された ACL 規則の一致基 準について、送信元IPアドレスおよび送信元マスクを指定します。 ACL規則のソースレイ ヤー4 ポートの一致基準は、port valueパラメータで指定します 。

<portvalue>には、domain、echo、ftp、ftpdata、http、smtp、snmp、telnet、tftp、wwwのキーワードを使用します。この値は同じポート番号に変換され、ポート範囲の開始および終了として使用されます。このコマンドにより*dstip*と*dstmask*パラメータで指定されたACL規則の一致基準について、宛先IPアドレスと宛先マスクを指定します。また、precedenceの一致状態やtos、tosmask、dscpパラメータを使用したDSCP値に応じて、ACL規則のTOSを指定します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.17.2.6 **no access-list**

このコマンドにより<*accesslistnumber*>パラメータで識別されたACLをシステムから削除します。

Syntax
no access-list {<1-99> | <100-199>} [<rule-id>]

<rule-id> -規則IDを追加します。

注: ACL番号は 1～199 の整数です。1～99 は通常のACLリスト、100～199 は拡張ACLリストです。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.17.2.7 **ip access-group**

このコマンドにより特定のアクセス制御リストをインターフェイスに付与します。

Syntax
ip access-group <1-199> in [<1-4294967295>]

<1-199> ACLの識別子。

<1-4294967295> ACLのシーケンス番号 。

初期設定

なし

コマンド・モード

グローバル・コンフィグ, インターフェイス・コンフィグ

9.18 CoSコマンド

9.18.1 Showコマンド

9.18.1.1 show queue cos-map

このコマンドにより特定インターフェイスの内部トラフィッククラスへマッピングされている、現在のDot1p (802.1p) プライオリティを表示します。slot/portパラメータは任意で、サービスマッピングの独立ポート単位クラスに対応しているプラットフォーム上のみで有効化されます。指定した場合、インターフェイスの802.1pマッピングテーブルが表示されます。指定しない場合、最新のグローバル設定が表示されます。

Syntax
show queue cos-map <slot/port>

<slot/port> はインターフェイス番号です。

初期設定

なし

コマンド・モード

特権EXEC, ユーザ EXEC /特権イネーブル、ユーザイネーブル

表示メッセージ

以下の情報は各ユーザプライオリティについて繰り返されます。

User Priority: 802.1pユーザプライオリティの値

Traffic Class: ユーザプライオリティがマップされるトラフィッククラスの内部キュー識別子

9.18.1.2 show queue ip-dscp-mapping

このコマンドにより内部トラフィッククラスにIP DSCPの値をマップします。<ipdscp>の値は 0～63 の整数のいずれか、またはキーワードaf11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、be、cs0、cs1、cs2、cs3、cs4、cs5、cs6、cs7、efのいずれかで指定されます。

<trafficclass>の値は 0～6 ですが、使用できるトラフィッククラスの数はプラットフォームにより異なります。

Syntax
show queue ip-dscp-mapping

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

IP DSCP: IP DSCP値

Traffic Class: キューマッピング

9.18.1.3 show queue trust

ACL規則は 2 つのオプションで作成されます。 ACL規則をフィルタするプロトコルに、 icmp、 igmp、ip、tcp、udpの使用を指定します。このコマンドによりsrcip and srcmask parametersで指定された ACL 規則の一致基 準について、送信元IPアドレスおよび送信元マスクを指定します。 ACL規則のソースレイ ヤー4 ポートの一致基準は、port valueパラメータで指定します 。

Syntax
show queue trust [<slot/port>]

<slot/port> はインターフェイス番号です。

初期設定

なし

コマンド・モード

特権EXEC, ユーザ EXEC /特権イネーブル、ユーザイネーブル

表示メッセージ

Class of Service Trust Mode: インターフェイスの信頼モード

Non-IP Traffic Class: 非IPトラフィックで使用さ れている トラフィック クラス。 COSトラストモードが「trust ip-dscp」または「trust ip-precedence」に設定されている場合にのみ表示されます 。

Untrusted Traffic Class: 信頼性がないすべてのトラフィックに使用す るトラフィッククラス。COSトラストモードが「untrusted」に設定されている場合にのみ表示されます 。

9.18.1.4 show queue cos-queue

このコマンドにより特定インターフェイスのclass-of-serviceキューの設定を表示します。slot/portパラメータは任意で、サービスマッピングの独立ポート単位クラスに対応しているプラットフォームのみで有効化されます。指定した場合、インターフェイスのサービスキューのクラス設定が表示されます。指定しない場合、最新のグローバル設定が表示されます。

Syntax
show queue cos-queue [<slot/port>]

<slot/port> はインターフェイス番号です。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Interface ： インターフェイスのスロット／ポートを表示します。グローバル設定を表示する場合、出力行にGlobal Configと表示されます。

Interface Shaping Rate: インターフェイスの最高送信帯域。インターフェイスのキュー単位の最高帯域の値には依存しません。値は設定可能です。

以下の値はインターフェイスの各キューについて繰り返されます。

Queue ID: インターフェイスが対応している、0～(n-1) の番号の付いたn個のキュー。nの値はプラットフォームに依存します。

Minimum Bandwidth: パーセンテージ表示の、キューの最低送信帯域保証。0 は帯域が保証されておらずキューが最大限で動作することを示します。値は設定可能です。

Scheduler Type: 絶対優先または重み付きスキームを使用し、このキューが予定通りに送信されるかを示します。

Queue Mgmt Type: このキューに使用されているキュー深度管理機能。テールドロップまたは重み付きランダム早期破棄 (WRED) 。値は設定可能です。

9.18.2 Configコマンド

9.18.2.1 queue cos-map

このコマンドにより 802.1pプライオリティをポート単位で内部トラフィッククラスにマップします。

Syntax
queue cos-map <priority> <queue-id> no queue cos-map

<priority> - キュープライオリティの範囲は 0～7

<queue-id> - マップ済みトラフィッククラスの範囲は 0～7

no - キュープライオリティと、マップ済みトラフィッククラスをデフォルトマッピングに戻します。



スタック可能接続ブレードのマップ済みトラフィッククラスの範囲は 0～6.

初期設定

なし

コマンド･モード

インターフェイス･コンフィグ.

このコマンドによりデバイスの内部トラフィッククラスに 802.1pプライオリティをマップします。

Syntax
queue cos-map all <priority> <queue-id> no queue cos-map all

<priority> - キュープライオリティの範囲は 0～7

<queue-id> - マップ済みトラフィッククラスの範囲は 0～7

no - キュープライオリティと、マップ済みトラフィッククラスをデフォルトマッピングに戻します。



スタック可能接続ブレードのマップ済みトラフィッククラスの範囲は 0～6.

初期設定

なし

コマンド･モード

グローバル·コンフィグ.

9.18.2.2 queue ip-dscp-mapping

このコマンドによりデバイスの内部トラフィッククラスにIP precedenceをマップします。

Syntax
queue ip-dscp-mapping <ipdscp> <queue-id> no queue ip-dscp-mapping

<ipdscp> - IP DSCPの値は 0～63 の整数のいずれか、またはIP DSCPキーワードaf11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、be、cs0、cs1、cs2、cs3、cs4、cs5、cs6、cs7、efのいずれかで指定されます。

<queue-id> - マップ済みトラフィッククラスの範囲は 0～7

no - IP DSCPと、マップ済みトラフィッククラスをデフォルトマッピングに戻します。



スタック可能接続ブレードのマップ済みトラフィッククラスの範囲は 0～6.

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.18.2.3 **queue trust**

このコマンドによりインターフェイスのサービストラストモードのクラスを設定します。モードはDot1p (802.1p)、IP Precedenceでtrustに設定することができます 。

Syntax
queue trust {dot1p | ip-dscp | untrusted} no queue trust

no - このコマンドによりインターフェイスのモードをデフォルト値に戻します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ.

このコマンドによりすべてのインターフェイスにサービストラストモードのクラスを設定します。モードはDot1p (802.1p)、IP Precedenceでtrustに設定することができます 。

Syntax
queue trust all {dot1p | ip-dscp | untrusted} no queue trust all

no -このコマンドによりすべてのインターフェイスのサービストラストモードのクラスをデフォルト値に戻します 。

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.18.2.4 queue cos-queue min-bandwidth

このコマンドにより各インターフェイスキューの最低送信帯域保証を指定します。

Syntax

```
queue cos-queue min-bandwidth <bw-0> <bw-1> … <bw-7>
no queue cos-queue min-bandwidth
```

<bw-0> <bw-1> … <bw-7> - 有効範囲は 0～100 で、5 ずつインクリメントし、合計値は 100 以下となります。

no − このコマンドにより各キューの最低帯域値をデフォルト値に戻します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ.

このコマンドによりデバイスの各インターフェイスキューの最低送信帯域保証を指定します。

Syntax

```
queue cos-queue min-bandwidth all <bw-0> <bw-1> … <bw-7>
no queue cos-queue min-bandwidth all
```

<bw-0> <bw-1> … <bw-7> - 有効範囲は 0～100 で、5 ずつインクリメントし、合計値は 100 以下となります。

no - このコマンドによりデバイスの各キューの最低帯域値をデフォルト値に戻します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.18.2.5 queue cos-queue strict

このコマンドにより各指定キューの絶対優先スケジューララモードをポート単位でアクティブ化します。

Syntax
queue cos-queue strict <queue-id-0> [<queue-id-1> … <queue-id-7>] no queue cos-queue strict <queue-id-0> [<queue-id-1> … <queue-id-7>]

<queue-id> - トラフィッククラスの範囲は 0 から 7 です。

no - このコマンドにより各指定キューをポート単位でデフォルトの重み付きスケジューララモードに戻します。.



スタック可能接続ブレードのマップ済みトラフィッククラスの範囲は 0〜6.

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ.

このコマンドによりデバイスの各指定キューの絶対優先スケジューララモードをアクティブ化します。

Syntax
queue cos-queue strict all <queue-id-0> [<queue-id-1> … <queue-id-7>] no queue cos-queue strict all <queue-id-0> [<queue-id-1> … <queue-id-7>]

<queue-id> - トラフィッククラスの範囲は 0 から 7 です。

no - このコマンドによりデバイスの各指定キューをポート単位でデフォルトの重み付きスケジューララモードに戻します。



スタック可能接続ブレードのマップ済みトラフィッククラスの範囲は 0〜6.

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.18.2.6 queue cos-queue traffic-shape

このコマンドによりインターフェイスの最高送信帯域制限値を指定します。レートシェーピングともいい、一時トラフィックバーストのオーバータイムをスムージングし、送信されたトラフィックレートがバウンドされます。

Syntax
queue cos-queue traffic-shape <bw> no queue cos-queue traffic-shape

<bw> - 有効範囲は 0～100 で、5 ずつインクリメントします。

no - このコマンドによりシェーピングレートの値をデフォルト値に戻します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ.

このコマンドによりすべてのインターフェイスの最高送信帯域制限値を指定します。レートシェーピングともいい、一時トラフィックバーストのオーバータイムをスムージングし、送信されたトラフィックレートがバウンドされます。

Syntax
queue cos-queue traffic-shape all <bw> no queue cos-queue traffic-shape all

<bw> - 有効範囲は 0～100 で、5 ずつインクリメントします。.

no - このコマンドによりすべてのインターフェイスのシェーピングレートの値をデフォルト値に戻します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.19 Stackコマンド

9.19.1 Showコマンド

9.19.1.1 show switch

このコマンドによりスタックシステム内のスタックメンバーの情報を表示します。スタッキング機能のあるEthernet接続ブレードのみで使用することができます。

Syntax
show switch [<unit>]

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

SW#: ユニットのID。スタックのユニット最大許可数は 8

ID: そのスイッチにあるインターフェイスを識別するために使われるユニットの識別子を表示します。

Role: ユニットがスタックマスターであるかスタックメンバーであるかを示します。

- Mgmt Switch
- Stack Member
- Unassigned

Mac Address: スイッチのMACアドレスを表示します。

Priority :スイッチのプライオリティは 0 から 15 の範囲、未割当て、または、無効化を表示します。

Current Status: スイッチにステータスを表示します。

- Ready
- Not Ready
- Unsupported
- Code Mismatch
- Config Mismatch
- Not Present
- Code Updating

Version: この欄はユニットに検出されたコードのバージョンを示す。

9.19.1.2 show switch stack port

このコマンドによりスタックシステム内のスタックメンバーのスタックポート情報を表示します。スタッキング機能のあるEthernet接続ブレードのみで使用することができます。

Syntax
show switch stack-port

初期設定

なし

コマンド･モード

特権EXEC

表示メッセージ

Unit: ユニットを表示する。.

Interface 所与のユニットにあるスタック可能インターフェイスを表示する。

Configured Stack Mode: 所与のインターフェイスに構成されたモードを表示する。 Currently, only N/A is displayed.

Running Stack Mode: スタック可能インターフェイスの実行時モードを表示する。

Link Status : スタッキングポートのリンクステータス (UP／DOWN)

Link Speed (Gb/s): スタック･ポートの最高速度を表示する。

9.19.1.3 show stack port counter statistic

このコマンドによりスタッキングポートの統計データを表示します。スタッキング機能のあるEthernet接続ブレードのみで使用することができます。

Syntax
show switch stack-port counters [detailed]

初期設定

なし

コマンド･モード

特権EXEC

表示メッセージ

Unit - ユニットを表示する。.

Interface - 所与のユニットにあるスタック可能インターフェイスを表示する。

送受信統計

Data Rate (Mb/s) - スタック･ポート上の速度概数を表示する。

Error Rate (Errors/s): スタック･ポート上のエラー頻度概数を表示する。

Total Errors -起動以降のエラー合計値を表示する。 カウンターはラップできる 。

9.19.2 Configコマンド

9.19.2.1 スイッチのプライオリティを設定する

このコマンドはスイッチのプライオリティを構成するために使われます。上位のプライオリティを持つスイッチは、スタックシステムのスタックマスターになる可能性がより高いです。

Syntax
switch <unit> priority <0-15> no switch <unit> priority

<unit> - 1 から 8 までのスイッチのユニット番号。

<0-15> - プライオリティの値。範囲は 0～15

no - このコマンドによりプライオリティの値をunassignedに戻します。

初期設定

Unassigned

コマンド・モード

グローバル・コンフィグ

9.19.2.2 switch provision

このコマンドは新しいスイッチを構成するために使います。ユーザーは物理スイッチがスタックシステムに結合される前にこのスイッチを事前に構成できます。

Syntax
switch <unit> provision no switch <unit> provision

<unit> - 1 から 8 までの範囲のスイッチのユニット番号

no - このコマンドはこのスイッチの構成を削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.19.2.3 switch movemanagement

このコマンドは管理スイッチをある移動するために使われます。

Syntax
switch movemanagement <fromunit> <tounit>

<fromunit> - 1 から 8 までの範囲のスイッチのユニット番号。

<tounit> - 1 から 8 までの範囲のスイッチのユニット番号。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

10　SNMPを使用する

はデバイスや他のネットワークの要素を特に管理するために設計された通信プロトコルです。SNMPで共通に管理されている装備には、スイッチ、ルータ、やホストコンピューターがあります。SNMPはこれらのデバイスを監視して性能を評価したり潜在的な障害を検出したり、さらにネットワーク環境で適切に動作するよう構成するために使われます。

SNMPによりネットワークの管理ステーションからこのスイッチへアクセスするには次の手順で行います。

1. ホストコンピュータ上に SNMP 管理アプリケーションをインストールします。
2. 管理ステーションとスイッチが同じ IP アドレスに構成されていることを確認します 。
3. SNMP からのネットワーク管理アクセスを行うため、コミュニティー名とアクセス権を設定します。
4. スイッチからトラップメッセージを受信するためには、トラップマネージャの IP アドレス、関連付けられたコミュニティー名、スイッチが作るトラップのタイプ等を特定しなければなりません。
5. SNMP 管理ステーションは管理情報ベース(MIB)に特定されているデバイスの変数の設定や読み取りにより、ネットワークのデバイスを構成し監視できます。このスイッチにサポートされているキーMIB グループは付録に記載されています。

デバイスのステータスを監視したり、ネットワーク管理システムからスイッチにあるシステムパラメータを変更するには、SNMP管理アプリケーションにより適当なMIB変数にアクセスできなければなりません。

10.1 対応MIB

標準MIBは以下のとおりです。

仕様	パブリックMIB名	MIBファイル
IEEE 802.1x	IEEE8021-PAE-MIB	dot1x.my
IEEE 802.3ad	LAG-MIB	dot3ad.my
RFC 1213	RFC1213-MIB	mib-2.my
RFC 2011	IP-MIB	RFC2011 ip-icmp.my
RFC 1493	BRIDGE-MIB	bridge.my
RFC 1643	ETHERLIKE-MIB	etherlike.my
RFC 1907	SNMPv2-MIB	v2-mib.my
RFC 2233	IF-MIB	if.my
RFC 2571	SNMP-FRAMEWORK-MIB	v3-arch.my
RFC 2572	SNMP-MPD-MIB	v3-mpd.my
RFC 2573	SNMP-TARGET-MIB	v3-tgt.my
RFC 2574	SNMP-USER-BASED-SM-MIB	v3-usm.my
RFC 2575	SNMP-VIEW-BASED-ACM-MIB	v3-acm.my
RFC 2576	SNMP-COMMUNITY-MIB	coex.my
RFC 2618	RADIUS-AUTH-CLIENT-MIB	radius_auth_client.my
RFC 2620	RADIUS-ACC-CLIENT-MIB	radius_acc_client.my
RFC 2674	P-BRIDGE-MIB Q-BRIDGE-MIB	pbridge.my vlan.my
RFC 2737	ENTITY-MIB	entity.my
RFC 2819	RMON-MIB	rmon.my
RFC 3289	DIFFSERV-MIB DIFFSERV-DSCP-TC	diffserv.my, diffserv_dscp_tc.my
RFC 2932	IANA-RTPROTO-MIB	rtproto.my
RFC 2668	MAU-MIB	rfc2668.my
RFC 2213	INTEGRATED-SERVICES-MIB	intserv.my
RFC 3291	INET-ADDRESS-MIB	inetaddress.my
RFC 1573	IANAifType-MIB	iftype.my
RFC 2677	IANA-ADDRESS-FAMILY-NUMBERS-MIB	ianaaddr.my

プライベートエンタープライズMIBは以下のとおりです。

プライベートMIB名	MIBファイル
FSC-SWITCH-MIB	fscref.my
OUTBOUNDTELNET-PRIVATE-MIB	telnet.my
MGMT-SECURITY-MIB	mgmt_security.my
DENIALOFSERVICE-PRIVATE-MIB	dos.my
COS-MIB	qos_cos.my
QOS-MIB	qos.my
QOS-ACL-MIB	qos_acl.my
QOS-DIFFSERV-EXTENSIONS-MIB	qos_diffserv_extensions.my
QOS-DIFFSERV-PRIVATE-MIB	qos_diffserv_private.my
RADIUS-CLIENT-PRIVATE-MIB	radius.my
RADIUS-ACC-CLIENT-MIB	radius_acc_client.my
RADIUS-AUTH-CLIENT-MIB	radius_auth_client.my
TACACS-CLIENT-MIB	tacacsclient.my
INVENTORY-MIB	inventory.my
LOGGING-MIB	logging.my
SNTP-CLIENT-MIB	sntp.my
SWITCHING-MIB	switching.my
PORTSECURITY-PRIVATE-MIB	portsecurity.my
SWITCHING-EXTENSION-MIB	switching_extension.my

10.2 MIBオブジェクトにアクセスする

MIBのオブジェクトはSNMPアプリケーションが制御と管理できるスイッチの機能を表します。一例は異なる変数をこのMIBグループで読み取ったり書き込んだりしてポート構成を取得したり設定できるRFC-2233 IF-MIBのグループです。このグループにサポートされる変数は下の表に記載されています。

RFC 2233 IF-MIB		
interfaces		
ifNumber	*Yes	*RO
ifMIBObjects		
ifTableLastChange	*No	RO
ifStackLastChange	No	RO
ifTable	Index:	ifIndex
ifDescr	Yes	RO
ifType	Yes	RO
ifMtu	Yes	RO
ifSpeed	Yes	RO
ifPhysAddress	Yes	RO
ifAdminStatus	Yes	*RW
ifOperStatus	Yes	RO
ifLastChange	Yes	RO
ifInOctets	Yes	RO
ifInUcastPkts	Yes	RO
ifInNUcastPkts	Yes	RO
ifInDiscards	Yes	RO
ifInErrors	Yes	RO
ifInUnknownProtos	No	RO
ifOutOctets	Yes	RO
ifOutUcastPkts	Yes	RO
ifOutNUcastPkts	Yes	RO
ifOutDiscards	No	RO
ifOutErrors	Yes	RO
ifOutQLen	No	RO
ifSpecific	No	RO
ifXTable	Index:	ifIndex
ifName	Yes	RO
ifInMulticastPkts	Yes	RO

ifInBroadcastPkts	Yes	RO
ifOutMulticastPkts	Yes	RO
ifOutBroadcastPkts	Yes	RO
ifHCInOctets	Yes	RO
ifHCInUcastPkts	Yes	RO
ifHCInMulticastPkts	Yes	RO
ifHCInBroadcastPkts	Yes	RO
ifHCOutOctets	Yes	RO
ifHCOutUcastPkts	Yes	RO
ifHCOutMulticastPkts	Yes	RO
ifHCOutBroadcastPkts	Yes	RO
ifLinkUpDownTrapEnable	Yes	RW
ifHighSpeed	Yes	RO
ifPromiscuousMode	Yes	RO
ifConnectorPresent	Yes	RO
ifAlias	No	RW
ifCounterDiscontinuityTime	Yes	RO
ifStackTable	Indicies:	ifStackHigherLayer, ifStackLowerLayer
ifStackStatus	No	*RC
ifRcvAddressTable	Indicies:	ifIndex, ifRcvAddressAddress
ifRcvAddressStatus	No	RC
ifRcvAddressType	No	RC
ifTestTable	Index:	ifIndex
ifTestId	No	RW
ifTestStatus	No	RW
ifTestType	No	RW
ifTestResult	No	RO
ifTestCode	No	RO
ifTestOwner	No	RW

***注記：**

Yes – 対応

No – 非対応

RW - 読み取り・書き込み可

RO - 読み取り専用

RC – 読み取り･作成可

10.3 対応トラップ

対応しているSNMPトラップは以下のとおりです。

RFC No	Title
RFC 1215	coldStart warmStart linkDown linkUp authenticationFailure
RFC 1493	newRoot topologyChange
RFC 2819	risingAlarm fallingAlarm

PRIMERGY
スイッチブレード (1Gbps 36/8+2) (PG-SW111)
スイッチブレード (1Gbps 36/12) (PG-SW112)
スイッチユーザーズガイド

CA92276-8603-02

発行日　2010年12月
発行責任　富士通株式会社